Computervredebreuk in politiesysteem Blue View door politiemol met Blue View-autorisatie

Voorde, J.M. ten

NJ 2022/54

Computervredebreuk in politiesysteem Blue View door politiemol met Blue View-autorisatie.

HR 30-11-2021, ECLI:NL:HR:2021:1691, m.nt. J.M. ten Voorde

Instantie
Hoge Raad (Strafkamer)
Datum
30 november 2021
Magistraten
Mrs. V. van den Brink, Y. Buruma, T. Kooijmans
Zaaknummer
20/01564
Conclusie
A-G mr. T.N.B.M. Spronken
Noot
J.M. ten Voorde
Folio weergave
Download gedrukte versie (PDF)
JCDI
JCDI:ADS634218:1
Vakgebied(en)
Materieel strafrecht / Delicten Wetboek van Strafrecht
Politierecht / Bijzondere onderwerpen
Brondocumenten
ECLI:NL:HR:2021:1691, Uitspraak, Hoge Raad (Strafkamer), 30-11-2021
ECLI:NL:PHR:2021:777, Conclusie, Hoge Raad (Advocaat-Generaal), 31-08-2021
Beroepschrift, Hoge Raad, 23-11-2020
Wetingang
Art. 138ab Sr

Essentie

Computervredebreuk in politiesysteem Blue View door politiemol met Blue View-autorisatie.
Het misbruik door de verdachte van zijn Blue View-autorisatie om informatie/gegevens over criminelen in te zien, deze informatie/gegevens over te nemen en deze informatie/gegevens aan deze criminelen te verstrekken, levert op het wederrechtelijk binnendringen in een geautomatiseerd werk m.b.v. een 'valse sleutel' cfm art. 138ab lid 1, onder c, Sr maar niet (zonder meer) het wederrechtelijk binnendringen door het aannemen van een 'valse hoedanigheid' cfm art. 138ab lid 1, onder d, Sr.

Samenvatting

Het hof heeft vastgesteld, dat de verdachte als politieambtenaar voorafgaand aan de bewezenverklaarde periode autorisatie heeft verkregen voor toegang tot het beveiligde politiesysteem Blue View, waartoe hij de beschikking had over een gebruikersnaam en een wachtwoord. Verder heeft het hof vastgesteld dat die autorisatie aan de verdachte was verstrekt om in het kader van zijn werk als politieambtenaar naspeuringen te verrichten, maar dat de verdachte het systeem vervolgens heeft bevraagd op gegevens over personen zonder dat daarvoor in de uitoefening van zijn politietaak enige aanleiding bestond. Op die manier kreeg de verdachte zonder daartoe onbevoegd inzage in gegevens en nam hij deze gegevens over. Op grond hiervan heeft het hof geoordeeld dat de verdachte zijn autorisatie voor toegang tot het systeem Blue View heeft 'misbruikt om informatie/gegevens over criminelen in te zien, deze informatie/gegevens over te nemen en deze informatie/gegevens ook aan deze criminelen te verstrekken'.
Het hof kon o.g.v. dit misbruik van die autorisatie oordelen dat de verdachte m.b.v. een 'valse sleutel' cfm art. 138ab lid 1, onder c, Sr een (deel van een) geautomatiseerd werk wederrechtelijk is binnengedrongen, mede in het licht van de

wetsgeschiedenis. 's Hofs oordeel dat de verdachte aldus ook door het aannemen van een 'valse hoedanigheid' cfm art. 138ab lid 1, onder d, Sr een (deel van een) geautomatiseerd werk wederrechtelijk is binnengedrongen, kan echter niet zonder meer uit de bewijsvoering worden afgeleid. De omstandigheid dat de verdachte met het misbruik van zijn autorisatie het door zijn collega's en de maatschappij in hem gestelde vertrouwen heeft geschonden, volstaat daartoe niet. De HR neemt daarbij in aanmerking dat niet blijkt dat de verdachte al een valse hoedanigheid had aangenomen toen hem de autorisatie werd verstrekt. Dit leidt echter niet tot cassatie omdat het weglaten van dit deel van de bewezenverklaring de aard en de ernst van het bewezenverklaarde in zijn geheel beschouwd niet aantast.

Partij(en)

Arrest op het beroep in cassatie tegen een arrest van het Gerechtshof 's-Hertogenbosch van 4 mei 2020, nummer 20-000736-18 (*NJFS* 2020/311; *red.*), in de strafzaak tegen [verdachte], adv.: mrs. R.J. Baumgardt, P. van Dongen en S. van den Akker, allen te Rotterdam.

Voorgaande uitspraak

Cassatiemiddel:

Middel II, zie 2.1; (*red.*).

Conclusie

Conclusie A-G mr. T.N.B.M. Spronken:

1. Het cassatieberoep

1.1.

De verdachte is door het Gerechtshof 's-Hertogenbosch bij arrest van 4 mei 2020 veroordeeld tot een gevangenisstraf voor de duur van vijf jaren wegens kortgezegd de volgende feiten:

- het meermalen (mede)plegen van schending van het ambtsgeheim[1.] (onder feit 1);
- het meermalen plegen van computervredebreuk[2.] (onder feit 2);
- ambtelijke omkoping[3.] (onder feit 3);
- gewoontewitwassen[4.] (onder feit 5) en
- het (meermalen) voorhanden hebben van een vals of vervalst reisdocument[5.] (onder feit 6).

Daarnaast heeft het hof de bijkomende straf opgelegd van ontzetting van het recht om een publiek ambt (als ambtenaar) te bekleden voor de duur van tien jaren en beslist omtrent het beslag, een en ander zoals nader bepaald in het arrest.

1.2.

De verdachte is in de media bekend geworden onder de naam 'politiemol [verdachte]' die ervan verdacht wordt dat hij als politieman jarenlang vertrouwelijke informatie heeft opgezocht in politiesystemen en die (tegen betaling) heeft gedeeld met personen uit het criminele circuit. Daarnaast wordt hem witwassen verweten en het voorhanden hebben van valse reisdocumenten.

1.3.

Er bestaat samenhang met de zaken 20/01532 en 20/01547, die betrekking hebben op de medeverdachten. In deze zaken zal ik vandaag ook concluderen.

1.4.

Het cassatieberoep is ingesteld namens de verdachte en mr. R.J. Baumgardt, P. van Dongen en S. van den Akker, advocaten te Rotterdam, hebben de volgende vier middelen van cassatie voorgesteld die ik achtereenvolgens zal bespreken:

(i) Het eerste middel komt op tegen de bewezenverklaring van feit 1, de schending van het ambtsgeheim.

(ii) Het tweede middel klaagt over de (bewezenverklaring en) kwalificatiebeslissing van feit 2, het plegen van computervredebreuk.

(iii) Het derde middel richt zich tegen de bewezenverklaring van feit 6, het voorhanden hebben van een vals reisdocument.

(iv) Het vierde middel klaagt erover dat het hof niet heeft gerespondeerd op het verweer dat ten aanzien van de

feiten 1 en 2 sprake is van eendaadse samenloop.

(…)

4. Middel II

4.1.

Het tweede middel komt op tegen de bewezenverklaring en kwalificatie van het onder feit 2 ten laste gelegde (meermalen) plegen van computervredebreuk en de verwerping van een daartoe strekkend dakdekkerverweer.[12.]

4.2.

Ten laste van de verdachte is onder 2 bewezenverklaard dat:

“hij in de periode van 1 januari 2012 tot en met 29 september 2015 in Nederland telkens, opzettelijk en wederrechtelijk in een of meer (delen van) geautomatiseerde werken, namelijk in een of meer (delen van) servers van de politie en/of de belastingdienst, is binnengedrongen met behulp van een valse sleutel en door het aannemen van een of meer valse hoedanigheid, namelijk door onbevoegd gebruik te maken van een gebruikersnaam en wachtwoord (voor de applicatie Blue View) en door zich met een gebruikersnaam en wachtwoord (voor de applicatie Blue View) toegang te verschaffen tot (delen van de) servers van de politie (waarop de applicaties Blue View en/of BVH en/of BVO en/of Summ-it en/of FIU waren geplaatst) met een ander doel dan waarvoor hem die gebruikersnaam en dat wachtwoord ter beschikking stonden en waarvoor hem die toegang was toegestaan, en (vervolgens) gegevens die waren opgeslagen en verwerkt en overgedragen door middel van (delen van) die geautomatiseerde werk(en) waarin hij zich wederrechtelijk bevond, voor zichzelf en anderen heeft overgenomen, namelijk door (telkens) (vertrouwelijke) informatie (omtrent een of meer personen en opsporingsonderzoeken) uit de applicatie Blue View op (een) gegevensdrager(s) en/of in (een) document(en) te plaatsen en/of(naar zichzelf) te mailen en/of te exporteren en/of (vervolgens) aan daartoe niet-gerechtigde personen te verstrekken;”

4.3.

Het bewezenverklaarde is door het hof gekwalificeerd als:

“computervredebreuk, terwijl de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt en worden overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf en een ander overneemt, meermalen gepleegd.”

4.4.

Het door het hof samengevatte verweer van de verdediging en de bewijsoverwegingen van het hof met betrekking tot feit 2 (voor zover niet al weergegeven onder 2.3) luiden als volgt:

“*Met betrekking tot feit 2: computervredebreuk*
De advocaat-generaal stelt zich op het standpunt dat dit feit bewezen kan worden verklaard.
Door de verdediging is vrijspraak bepleit. Daartoe heeft zij — kort gezegd — het volgende aangevoerd. Er is geen sprake van het zogenaamd ‘hacken’ zoals bedoeld in artikel 138ab Wetboek van Strafrecht. De rechtbank heeft het begrip ‘binnendringen’ verkeerd uitgelegd. Dit artikel strekt zich namelijk niet tot de bescherming van de (inhoud van) gegevens, maar is bedoeld om het binnendringen op zich strafbaar te stellen. Dit blijkt des te meer uit het nieuwe artikel 138c Wetboek van Strafrecht, in welk artikel het met rechtmatig toegang wederrechtelijk overnemen van gegevens strafbaar is gesteld. Van dergelijk binnendringen is thans geen sprake, nu verdachte beschikte over een rechtmatige 'sleutel', te weten zijn accreditatie om Blue View te raadplegen. Bovendien is geen sprake van een valse hoedanigheid, doorbreken van beveiliging of technische ingreep van de zijde van verdachte, aldus de verdediging.
Het hof stelt, onder verwijzing naar artikel 80sexies Sr zoals geldend ten tijde van het tenlastegelegde, samen met de rechtbank vast dat — zoals bij de bespreking van feit 1 aan de orde is geweest — het Blue View systeem een geautomatiseerd werk is, in casu zijnde een digitaal verzamelsysteem dat door politieambtenaren in de uitoefening van hun politietaak kan worden geraadpleegd mits zij daarvoor zijn geaccrediteerd en beschikken over een autorisatie. Er moeten om in het beveiligde systeem te komen een gebruikersnaam (dienstnummer) en wachtwoord worden gegeven. Verdachte beschikte over een zodanige autorisatie vanaf 29 augustus 2011 tot zijn aanhouding op 29 september 2015.
Het hof overweegt omtrent het verweer dat verdachte rechtmatig beschikte over een autorisatie waarmee hij Blue View kon raadplegen en dat daarmee geen veroordeling ter zake van het onder 2 tenlastegelegde kan volgen, als volgt.
Artikel 138ab
1. Met gevangenisstraf van ten hoogste twee jaren geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:
a. door het doorbreken van een beveiliging,
b. door een technische ingreep,

c. met behulp van valse signalen of een valse sleutel, of

d. door het aannemen van een valse hoedanigheid.

2. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt.

Het schenden van artikel 138ab Sr was tot de inwerkingtreding van de Wet kraken en leegstand (*Stb.* 2010, 320) tot 1 oktober 2010 geregeld in art. 138a Sr. Op grond van de parlementaire stukken kan ter zake van het huidige art. 138ab Sr — het toenmalige art. 138a Sr — het volgende worden opgemerkt.

De strafbaarstelling van art. 138ab Sr beschermt degene die blijkens feitelijke beveiliging heeft duidelijk gemaakt dat hij zijn gegevens heeft willen afschermen tegen nieuwsgierige blikken door het systeem daartegen te beveiligen. De bescherming van gerechtvaardigde belangen van houders van gegevensbestanden die, opgeslagen in computers, vooral via de telecommunicatie-infrastructuur voor onbevoegde blikken toegankelijk zijn, wordt via deze strafbaarstelling geboden doordat het doorbreken van een aangebrachte beveiliging wordt strafbaar gesteld. Daarbij is aansluiting gezocht bij de bestaande strafbaarstelling betreffende de huisvredebreuk. De eisen rondom wederrechtelijke binnendringing zijn in de sfeer van de informatietechniek in deze strafbaarstelling vertaald in het bestanddeel ‘binnendringen’, inhoudende dat een beveiliging moet zijn doorbroken. In de Memorie van Toelichting is hierover opgenomen: ‘Het gaat er om dat de degeen die de computer binnendringt door het doorbreken van de beveiliging, heeft blijk gegeven de wetenschap te hebben gehad dat hij een beveiligd systeem binnendringt en doelbewust enige inspanning heeft gedaan de beveiliging te doorbreken’ (vgl. *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 16).

Het aangehaalde lid 1 van artikel 138ab Sr geeft aan dat van ‘binnendringen’ in ieder geval sprake is indien de toegang tot het werk wordt verworven met behulp van een valse sleutel of door het aannemen van een valse hoedanigheid. In de Kamerstukken van het toenmalige wetsvoorstel wordt over het bestanddeel ‘valse sleutel’ weergegeven dat een password een sleutel is die de gebruiker toegang geeft tot het systeem of tot een deel daarvan. Daarbij werd aangehaald dat de Hoge Raad in zijn arrest van 20 mei 1986, ECLI:NL:HR:1986:AC9359, *NJ* 1987/130) heeft bepaald dat een huissleutel die wordt gebruikt tot opening van een slot door iemand die daartoe niet is gerechtigd, een valse sleutel is en dat niet is vereist dat ten aanzien van de sleutel enige beveiligingsmaatregel is genomen. Onder verwijzing naar artikel 90 Sr, waarin geen definitie van het begrip ‘valse sleutels’ wordt gegeven maar enkel wordt aangegeven wat onder het begrip dient te worden begrepen (‘alle tot opening van het slot niet bestemde werktuigen’) — waarbij de wetgever heeft aangegeven dat '(O)nverschillig (is) of het werktuig al of niet een sleutel, zoo het slechts niet die sleutel is, die voor opening van dat slot bestemd is.' (zie H.J. Smidt, Geschiedenis van het Wetboek van Strafrecht, Deel I, tweede druk, p. 544) — stelt het hof dat de jurisprudentie van de Hoge Raad verder ter zake van ‘valse sleutel’ heeft uitgemaakt dat ook onrechtmatig gebruik van bijvoorbeeld een bankpas of een tankpas kan worden aangemerkt als het gebruik maken van een ‘valse sleutel’. Anders gezegd: de Hoge Raad geeft een ruime uitleg aan het begrip ‘valse sleutels’ waarbij ook gebruik door een onbevoegde als een ‘valse sleutel’ kan worden aangemerkt (vgl. CAG Knigge in ECLI:NL:PHR:2017:1012 onder verwijzing naar HR 3 oktober 2017, ECLI:NL:HR:2017:2546).

Voor wat betreft de uitleg in de genoemde bepaling ter zake van het bestanddeel ‘valse hoedanigheid wijst het hof op de uitleg die de Hoge Raad daaraan geeft in zijn overzichtsarrest van 20 december 2016, ECLI:NL:HR:2016:2892, *NJ* 2017/158, m.nt. Keijzer, rov. 2.3.4. De Hoge Raad heeft ter zake van het aannemen van een valse hoedanigheid overwogen dat het daarbij in de kern gaat om dat het handelen van de verdachte ertoe kan leiden dat bij de ander een onjuiste voorstelling van zaken in het leven wordt geroepen met betrekking tot de 'persoon' van de verdachte wat betreft diens hoedanigheid, waarbij die onjuiste voorstelling van zaken in het leven wordt geroepen teneinde daarvan misbruik te maken. Daarbij heeft de Hoge Raad specifiek aangegeven dat de in de rechtspraak wel gebruikte formulering dat een verdachte zich als een 'bonafide' deelnemer aan het rechtsverkeer heeft gepresenteerd, met betrekking tot het aannemen van een valse hoedanigheid slechts relevant is als zo een presentatie als bonafide (potentiële) wederpartij berust op voldoende specifieke gedragingen die in de desbetreffende context erop zijn gericht bij het beoogde slachtoffer een onjuiste voorstelling van zaken in het leven te roepen teneinde daarvan misbruik te maken.

De verdachte heeft op enig moment, namelijk toen hij werkzaam zou worden bij de Nationale Recherche toegang gekregen tot het beveiligde Blue View systeem. Om Blue View te kunnen raadplegen, heeft verdachte moeten inloggen met een gebruikersnaam (zijn dienstnummer) en een wachtwoord. Daarmee verkreeg verdachte ook de bevoegdheid om de resultaten van bevragingen te kunnen exporteren als PDF of Excel-bestand en op te slaan op een bijvoorbeeld een externe opslagplaats, zoals een USB stick. Verdachte werd daarbij uitdrukkelijk via het systeem gewaarschuwd dat oneigenlijk gebruik dan wel misbruik van deze gegevens, waaronder het verstrekken van deze gegevens aan derden welke niet de vereiste autorisatie bezitten, ten strengste verboden was. Zoals hierboven weergegeven zijn deze werkzaamheden spoedig gestaakt omdat hij geen 'Verklaring van geen bezwaar' verkreeg. Desalniettemin heeft verdachte nog jaren dit systeem ingezien.

Het hof oordeelt dat verdachte op grond van de in het voorgaande weergegeven feiten en omstandigheden het beveiligde politiesysteem Blue View, dat hij in het kader van zijn specifieke werkzaamheden als politieambtenaar op die betreffende gegevens niet behoefde en niet behoorde in te zien, heeft misbruikt om informatie/gegevens over criminelen in te zien, deze

informatie/gegevens over te nemen en deze informatie/gegevens ook aan deze criminelen te verstrekken. Hij is met behulp van de aan hem toegekende autorisatie het systeem Blue View opzettelijk en wederrechtelijk binnengedrongen om inzage te krijgen van gegevens waar hij niet toe bevoegd was en vervolgens deze over te nemen. Door op deze wijze de betreffende gegevens in te zien en over te nemen, heeft verdachte, wetende dat het een beveiligd systeem betrof, doelbewust de beveiliging van dit systeem doorbroken en is hij derhalve het systeem binnengedrongen. Hij heeft zich daarbij bediend van een valse sleutel en het aannemen van een valse hoedanigheid. Verdachte heeft immers weliswaar geautoriseerd maar onbevoegd ter zake van de betreffende gegevens zich opzettelijk en wederrechtelijk de toegang verschaft tot het systeem Blue View. Daarbij was aan verdachte de autorisatie verstrekt om het systeem te raadplegen om in het kader van zijn werk als politieambtenaar naspeuringen te verrichten, maar niet om daarmee informatie in te winnen en dit aan criminelen te verstrekken waardoor deze zich aan die naspeuringen konden onttrekken. Tevens heeft verdachte in de context van zijn handelen als politieambtenaar voldoende specifieke gedragingen verricht om een onjuiste voorstelling van zaken in het leven roepen met betrekking tot de hoedanigheid van de 'persoon' van de verdachte. Verdachte heeft namelijk onder de voorstelling van de hoedanigheid van een persoon die gerechtigd was om op grond van zijn werkzaamheden inzage in de betreffende gegevens te mogen verrichten, zich de toegang verschaft tot het systeem Blue View, teneinde daarvan misbruik te maken. Verdachte bevroeg vele personen in het Blue View systeem zonder dat is gebleken dat daartoe in de uitoefening van zijn politietaak enige aanleiding bestond. Zowel de collega's van verdachte als de maatschappij mocht erop vertrouwen — mede gelet de aard en de functie van verdachte en de ambtseed die hij heeft moeten afleggen — dat zij te maken hadden met een betrouwbare en onkreukbare ambtenaar. Verdachte heeft echter op bedrieglijke wijze misbruik gemaakt van het vertrouwen van en in de politie.
Anders dan de verdediging is het hof van mening dat de strafbaarstelling opgenomen in artikel 138c Sr geen inbreuk maakt op een mogelijke bewezenverklaring van hetgeen aan verdachte onder 2 is tenlastegelegd en strafbaar is gesteld onder artikel 138ab Sr. De wetgever heeft in artikel 138c Sr strafbaar gesteld het opzettelijk en wederrechtelijk voor zichzelf of voor een ander overnemen van niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk. De bepaling is vooral van belang voor gevallen waarin de dader rechtmatige toegang heeft tot de gegevens, maar deze wederrechtelijk overneemt (vgl. *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 64). In de onderhavige zaak had verdachte weliswaar autorisatie om toegang te krijgen tot het systeem Blue View, maar hij was niet bevoegd tot het inzien en overnemen van de gegevens waar het in de onderhavige strafzaak om gaat. Verdachte heeft derhalve met behulp van de aan hem toegekende autorisatie het systeem Blue View opzettelijk en wederrechtelijk binnengedrongen om inzage te krijgen van gegevens waar hij niet toe bevoegd was en vervolgens deze overgenomen.
Het hof is dan ook van oordeel dat de tenlastegelegde computervredebreuk bewezen kan worden verklaard."

5. Beoordeling van het tweede middel

5.1.

Het middel bevat twee klachten:

(i) In de eerste plaats wordt geklaagd dat het oordeel van het hof dat de verdachte onrechtmatig het beveiligde politiesysteem is binnengedrongen en zich daarbij bediend heeft van een valse sleutel en een valse hoedanigheid, van een onjuiste rechtsopvatting getuigt, althans onvoldoende met redenen is omkleed omdat de verdachte geautoriseerd was Blue View te raadplegen.

(ii) De tweede klacht — die enigszins samenhangt met de eerste klacht — gaat over het verweer van de verdediging dat er vanwege de autorisatie van de verdachte om Blue View te raadplegen, geen sprake is geweest van 'hacken' oftewel onrechtmatig binnendringen zoals strafbaar gesteld in art. 138ab Sr. Daarbij heeft de verdediging zijdelings gewezen op de op 1 maart 2019 ingevoerde aparte strafbaarstelling in art. 138c Sr,[13.] welke bepaling ná de tenlastegelegde feiten in werking is getreden en die geschreven is voor de gevallen waarin de dader rechtmatige toegang heeft tot een geautomatiseerd werk, maar daar vervolgens onrechtmatig gebruik van maakt. Nu wordt in cassatie[14.] door de stellers van het middel een beroep gedaan op het lex mitior-beginsel. Dit beginsel komt erop neer dat indien na het begaan van een feit, door een gewijzigd inzicht van de wetgever over de strafwaardigheid van dit feit, de delictsomschrijving in voor de verdachte gunstige zin is gewijzigd, art. 1 lid 2 Sr met zich brengt, dat de gunstigere nieuwe bepaling op de verdachte moet worden toegepast. Betoogd wordt dat het hof in de onderhavige zaak ten aanzien van de kwalificatiebeslissing en/of strafoplegging de voor verdachte gunstigere bepaling van artikel 138c Sr had moeten toepassen[15.] en dat nu het hof dat niet heeft gedaan de kwalificatiebeslissing/strafoplegging onvoldoende met redenen is omkleed.

De tweede klacht

5.2.

Ik zal eerst ingaan op de tweede klacht, het beroep op het lex mitior-beginsel, omdat ik hierover kort kan zijn. Deze klacht kan mijns inziens niet slagen vanwege het volgende.

5.3.

Art. 138ab en 138c Sr luid(d)en als volgt:

"Art. 138ab

1. Met gevangenisstraf van ten hoogste twee jaren geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:

a. door het doorbreken van een beveiliging,

b. door een technische ingreep,

c. met behulp van valse signalen of een valse sleutel, of

d. door het aannemen van een valse hoedanigheid.

2. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt.

Art. 138c Sr (sinds 1 maart 2019 tot 1 mei 2021)Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die opzettelijk en wederrechtelijk niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk, voor zichzelf of voor een ander overneemt.

Art. 138c Sr (sinds 1 mei 2021)1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die opzettelijk en wederrechtelijk niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk, voor zichzelf of voor een ander overneemt of doorgeeft.

2. Indien de gegevens een niet-contant betaalinstrument betreffen, wordt de schuldige gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.

3. Indien het feit wordt gepleegd met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, wordt de schuldige gestraft met gevangenisstraf van ten hoogste drie jaren of geldboete van de vierde categorie."

5.4.

Het lex mitior-beginsel is in onderhavige zaak niet van toepassing omdat art. 138c Sr geen nieuwe strafbaarstelling is die voortvloeit uit een gewijzigd inzicht van de wetgever over de strafwaardigheid van hetgeen is strafbaar gesteld in art. 138ab Sr.[16.]Art. 138c Sr heeft betrekking op het wederrechtelijk overnemen van gegevens opgeslagen in een geautomatiseerd werk ongeacht of sprake is van wederrechtelijke toegang. Het wederrechtelijk overnemen van gegevens bij *rechtmatige toegang* was voor de invoering van dit artikel niet strafbaar gesteld. Art. 138ab Sr, dat ook na de invoering van art. 138c Sr is blijven bestaan, stelt allereerst *het binnendringen* van het geautomatiseerde werk (computervredebreuk, lid 1) strafbaar, alsmede het (eventueel) vervolgens overnemen van gegevens daaruit (lid 2). Het essentiële verschil tussen beide bepalingen is dus of sprake is geweest van rechtmatige toegang alvorens de gegevens wederrechtelijk te gebruiken. Van een gewijzigd inzicht in de strafwaardigheid van hetgeen strafbaar is gesteld in art. 138ab Sr (en voorheen in art. 138a Sr) is dus geen sprake. Daarmee is overigens de vraag of het hof kon oordelen dat de verdachte, gebruikmakend van zijn autorisatie, de politiesystemen is binnengedrongen nog niet beantwoord. Daarover gaat de eerste klacht.

5.5.

De tweede klacht faalt.

De eerste klacht

5.6.

Bij de eerste klacht draait het om de vraag of de verdachte, op het moment dat hij de litigieuze bevragingen in Blue View deed, dit systeem wederrechtelijk is binnengedrongen in de zin van art. 138ab Sr.

5.7.

Het hof heeft geoordeeld dat dit het geval was, ondanks dat hij toegang had tot het beveiligde Blue View systeem en daartoe een gebruikersnaam en wachtwoord had gekregen en tevens de bevoegdheid had om de resultaten van bevragingen te exporteren en op te slaan. De reden dat het hof tot de conclusie komt dat hij desalniettemin het Blue View systeem opzettelijk en wederrechtelijk is binnengedrongen, is gelegen in de omstandigheid dat hij vanwege zijn specifieke werkzaamheden binnen de politie, die gegevens niet hoefde en niet behoorde in te zien.

Deze omstandigheden zijn tevens aanleiding voor het hof om aan te nemen dat de verdachte zich heeft bediend van een valse sleutel omdat de autorisatie er niet toe strekte (buiten zijn specifieke werkzaamheden) informatie in te winnen en aan criminelen te verstrekken. Ook heeft het hof geoordeeld dat de verdachte daarbij een valse hoedanigheid heeft aangenomen omdat hij “onder de voorstelling van de hoedanigheid van een persoon die gerechtigd was om op grond van zijn werkzaamheden inzage in de betreffende gegevens te mogen verrichten, zich de toegang [heeft] verschaft tot het systeem Blue View, teneinde daarvan misbruik te maken”.

5.8.

Volgens de stellers van het middel getuigt dit oordeel van het hof van een onjuiste uitleg van de termen “binnendringen”, “valse sleutel” en het aannemen van een “valse hoedanigheid” in de zin van art. 138ab Sr. Kort samengevat wordt hiertoe gesteld dat in art. 138ab Sr het zogenaamde “hacken” oftewel de computerinbraak strafbaar wordt gesteld en dat van binnendringen slechts sprake kan zijn als de beveiliging van een systeem wordt doorbroken en daartoe ook bewuste inspanningen zijn gedaan. Van binnendringen door gebruikmaking van een valse sleutel is volgens de stellers van het middel geen sprake omdat de verdachte rechtmatig beschikte over een accreditatie. Ook heeft de verdachte geen valse hoedanigheid aangenomen, omdat hij zich niet heeft voorgedaan als een ander maar onder zijn eigen gegevens heeft ingelogd en als zodanig herkenbaar was.

5.9.

Centraal staat in deze klacht of in onderhavige zaak sprake is geweest van “binnendringen” in de zin van art. 138a Sr. Daarnaast speelt de kwestie of het hof bij de begrippen “valse sleutel” en “het aannemen van een vals hoedanigheid” het juiste toetsingskader heeft gehanteerd. Hoewel de drie betrokken bestanddelen met elkaar samenhangen, het gebruik van een valse sleutel of het aannemen van een valse hoedanigheid zijn als het ware middelen waarmee kan worden binnengedrongen, heb ik ervoor gekozen eerst te onderzoeken of het hof ten aanzien van de begrippen “valse sleutel” en “het aannemen van een “valse hoedanigheid” (art. 138ab, lid 1 onder c en d) van een juiste rechtsopvatting is uitgegaan. Daarna zal ik ingaan op de vraag of het hof terecht heeft geoordeeld dat in onderhavige zaak sprake is van wederrechtelijk binnendringen in een geautomatiseerd werk. Daarbij zal ik aan de hand van de wetsgeschiedenis en de jurisprudentie ook aandacht besteden aan het karakter en de ratio van de strafbaarstelling van art. 138ab Sr.

Valse sleutel

5.10.

Ten aanzien van het gebruik van een valse sleutel is tijdens de behandeling van het wetsvoorstel Wet computercriminaliteit in het artikelsgewijs commentaar in de Memorie van Antwoord bij het voorgestelde art. 138a (de voorloper van art. 138ab Sr) door de minister het volgende opgemerkt:

“Ik ga er daarbij vanuit dat een password een sleutel is die de gebruiker toegang geeft tot het systeem of tot een deel daarvan. Bij arrest van de Hoge Raad van 20 mei 1986 (*NJ* 1987, 130) is vastgesteld dat een huissleutel die wordt gebruikt tot opening van een slot door iemand die daartoe niet is gerechtigd, een valse sleutel is. Niet is vereist dat ten aanzien van de sleutel enige beveiligingsmaatregel is genomen. Voldoende is dat de sleutel tegen de wil van de rechthebbende uit zijn macht is verloren gegaan. De kraker die een password van een bulletin–board haalt en daarmee een computer kraakt, is dus strafbaar zelfs indien de beheerder van de computer weet dat het password daar beschikbaar is en nalatig is geweest de beveiliging aan te passen.”[17.]

5.11.

Van belang is ook de volgende passage uit die Memorie van Antwoord:

“Met de voorgestelde nota van wijziging wordt echter ook het zonder enige inspanning halen van een password van een bulletinboard en het vervolgens aanwenden bij het betrokken bedrijf strafbaar ingevolge deze bepaling. Deze drempel is zelfs lager dan wordt voorgesteld in de brief, daar ook de gemiddelde computerkraker in deze omstandigheden zonder enige inspanning kan binnendringen.”[18.]

5.12.

Duidelijk is dus dat in de wet(sgeschiedenis) aansluiting wordt gezocht bij de definitie van valse sleutel zoals die bij niet-digitale delicten geldt en is gedefinieerd in art. 90 Sr. Deze bepaling wordt in de rechtspraak ruim uitgelegd. Zo is de huissleutel die uit een tas van de eigenaar is gestolen en gebruikt is voor de opening van de toegangsdeur voor het huis door de Hoge Raad aangemerkt als ‘valse sleutel’:

“Een huissleutel welke tot opening van het slot van de toegangsdeur van een woning wordt gebruikt door iemand die daartoe geen recht heeft, is ten aanzien van dat slot een valse sleutel.”[19.]

Datzelfde geldt voor een pinpas waarvan met de bijbehorende pincode wederrechtelijk geld is gepind.[20.]

5.13.

Het hof, dat voormelde jurisprudentie in zijn arrest aanhaalt, is dan ook ten aanzien van het begrip “valse sleutel” van het juiste toetsingskader uitgegaan. Op de vraag of dit in onderhavige zaak er ook toe leidt dat er sprake is geweest van “binnendringen” in de zin van art. 138ab Sr, zoals het hof heeft geoordeeld, kom ik hierna nog terug.

Valse hoedanigheid

5.14.

Over het aannemen van een valse hoedanigheid in de betekenis van art. 138a (oud) of 138ab Sr is in de wetsgeschiedenis niets te vinden. Aangenomen mag echter worden dat, net als ten aanzien van de valse sleutel, dient te worden aangesloten bij de uitleg daarvan bij niet-digitale delicten, in dit geval de valse hoedanigheid bij oplichting. Het hof heeft, meen ik, dan ook terecht de uitleg die de Hoge Raad daaraan geeft in zijn overzichtsarrest van 20 december 2016,[21.] tot uitgangspunt genomen. De Hoge Raad heeft daarin overwogen dat het bij het aannemen van een valse hoedanigheid er in de kern om gaat, dat het handelen van de verdachte ertoe kan leiden dat bij de ander een onjuiste voorstelling van zaken in het leven wordt geroepen met betrekking tot de 'persoon' van de verdachte wat betreft diens hoedanigheid, waarbij die onjuiste voorstelling van zaken in het leven wordt geroepen teneinde daarvan misbruik te maken. Daarbij heeft de Hoge Raad specifiek aangegeven dat de in de rechtspraak wel gebruikte formulering dat een verdachte zich als een 'bonafide' deelnemer aan het rechtsverkeer heeft gepresenteerd, met betrekking tot het aannemen van een valse hoedanigheid slechts relevant is als zo een presentatie als bonafide (potentiële) wederpartij berust op voldoende specifieke gedragingen die in de desbetreffende context erop zijn gericht bij het beoogde slachtoffer een onjuiste voorstelling van zaken in het leven te roepen teneinde daarvan misbruik te maken. Ook hier geldt dat ik van mening ben dat het hof het juiste toetsingskader heeft aangelegd en dat ik er nog op terugkom of het hof dit toetsingskader in onderhavige zaak op een juiste wijze heeft toegepast bij de vaststelling dat in casu sprake is geweest van “binnendringen” in de zin van art. 138ab Sr.

Binnendringen

5.15.

Dan kom ik nu toe aan de aan de betekenis van de term “binnendringen”. Uit de wetsgeschiedenis komt naar voren dat het bij computervredebreuk, achtereenvolgens strafbaar gesteld in art. 138a (oud) Sr en in art. 138ab Sr, gaat om het wederrechtelijk binnendringen (hacken) van een geautomatiseerd werk. Daarbij is aansluiting gezocht bij de strafbepaling en systematiek van niet-digitale delicten, zoals huisvredebreuk (art. 138 Sr). Bij de strafbaarstelling van computervredebreuk staat de bescherming van het geautomatiseerd werk, ook wel aangeduid als ‘de huls’, voorop en niet zozeer de gegevens die daarin zijn opgeslagen.[22.] Het inzien of bekijken van bepaalde gegevens wordt pas strafbaar als de huls waarin die gegevens zijn opgeslagen, wederrechtelijk wordt binnengedrongen. Dat is het geval als de beheerder of de rechthebbende er nadrukkelijk voor gezorgd heeft dat gegevens die niet bestemd zijn voor ogen van vreemden zijn afgeschermd of beveiligd.[23.] In het oorspronkelijke wetsvoorstel Computercriminaliteit was dan ook een beveiligingseis voorgesteld. Bij binnendringen moest sprake zijn van enige beveiliging die moest worden doorbroken:

“Het [de strafbepaling, AG TS] beschermt degeen die blijkens feitelijke beveiliging heeft duidelijk gemaakt dat hij zijn gegevens heeft willen afschermen tegen nieuwsgierige blikken. Het gaat hierbij om een uitwerking van het beginsel dat het medium wordt beveiligd.”[24.]

5.16.

Aan die die feitelijke beveiliging hoefde overigens niet zwaar te worden getild:

“Het gaat er om dat de degeen die de computer binnendringt door het doorbreken van de beveiliging, heeft blijk gegeven de wetenschap te hebben gehad dat hij een beveiligd systeem binnendringt en doelbewust enige inspanning heeft gedaan de beveiliging te doorbreken. (…) Het kan voor bedrijven geen bezwaar zijn aan te tonen dat zij ten minste enige reële beveiliging hebben, al was het maar dat zij een systeem van autorisatie hebben wat betreft de verlening van toegang. Een dergelijk systeem is algemeen bekend.”[25.]

5.17.

Volgens Knigge blijkt hieruit dat in het oorspronkelijke wetsvoorstel Computercriminaliteit "een systeem van autorisatie" in beginsel als een reële beveiliging werd beschouwd.[26.] Het onbevoegd gebruik van het juiste wachtwoord zou dan al als het binnendringen in een daartegen beveiligd werk moeten worden aangemerkt. Tijdens het wetgevingsproces werd echter kritiek geuit op de beveiligingseis en hoe deze in de memorie van toelichting werd uitgelegd. Het wetsvoorstel werd daarom gewijzigd. Daarbij werd de beveiligingseis afgezwakt omdat ook op andere manieren sprake kon zijn van binnendringen:

“Artikel 138a stelt in zijn nieuw voorgestelde vorm strafbaar elke vorm van binnendringen, zowel wanneer daartoe een beveiliging is doorbroken, als wanneer een valse sleutel, bij voorbeeld een password, een valse hoedanigheid of listige kunstgrepen zijn aangewend. De straffeloosheid wordt daardoor beperkt tot de gevallen dat geen enkele beveiliging op een geautomatiseerd werk is aangebracht.”[27.]

5.18.

Bij de invoering van de Wet computercriminaliteit II in 2006 werd nog minder nadruk gelegd op de beveiligingseis en kwam die als algemene noodzakelijke voorwaarde te vervallen. Gekozen werd voor een niet-limitatieve omschrijving van verschillende wijzen van binnendringen die te vinden is in het huidige art. 138ab lid 1 onder a t/m d Sr. Van binnendringen is

sprake als het gaat (a) om de doorbreking van een beveiliging, (b) door een technische ingreep, (c) het gebruik van valse signalen of een valse sleutel of (d) het aannemen van een valse hoedanigheid. De wetgever heeft het aan de rechtspraktijk overgelaten welke andere manieren van binnendringen binnen de delictsomschrijving kunnen vallen.[28.]

5.19.

Omdat het in deze zaak gaat om een verdachte die weliswaar een autorisatie had maar volgens het oordeel van het hof onbevoegd was bepaalde gegevens te raadplegen binnen het geautomatiseerd werk, wijs ik nog op de volgende passage uit de wetsgeschiedenis. Hieruit kan worden afgeleid dat alleen al de *overschrijding* van een autorisatie die verleend is voor *delen* van een geautomatiseerd volgens de wetgever computervredebreuk kan opleveren. In de Memorie van Antwoord bij de Wet Computercriminaliteit I verwoordt de minister dit onder meer als volgt (p. 30):

"Ik wijs erop dat het voorgestelde artikel 138a ook ziet op onderdelen van een computer. Indien een gebruiker slechts is geautoriseerd tot kennisneming van bepaalde gegevens, en hij slaagt erin op één van de strafbaar gestelde wijzen toegang te krijgen tot een ander onderdeel van de computer, en daarmee tot andere gegevens, maakt hij zich schuldig aan overtreding van het voorgestelde artikel 138a. Heeft geen beveiliging plaatsgevonden — dit ligt in de vrijheid van de beheerder van een informatiesysteem — dan is dit toegestaan, althans niet strafbaar."

5.20.

Mede in het licht van de ontwikkelingen die de strafbepaling heeft doorgemaakt — waarbij de beveiligingseis op de achtergrond is geraakt — is de huidige betekenis die aan deze passage uit de wetsgeschiedenis moet worden toegekend betrekkelijk en bovendien voor tweeërlei uitleg vatbaar. Enerzijds wordt de suggestie gewekt dat indien een gebruiker, die autorisatie heeft tot kennisneming van bepaalde gegevens, zich toegang verschaft tot gegevens waartoe hij niet bevoegd is, strafbaar is. Anderzijds wordt gesteld dat deze gegevens wel beveiligd moeten zijn. Onduidelijk is of daarmee een algemene beveiliging wordt bedoeld, die na het passeren daarvan zowel toegang geeft tot gegevens waartoe de gebruiker bevoegd is als waartoe hij onbevoegd is, of dat het gaat om een aparte nadere beveiliging van het onderdeel van het geautomatiseerde systeem waarvoor de gebruiker niet bevoegd is. Daar komt nog bij dat, zoals gezegd, de beveiligingseis thans niet meer als *noodzakelijke* voorwaarde wordt gesteld, maar onder één van de in art. 138ab Sr genoemde wijzen van binnendringen, namelijk het in art. 138ab sub a genoemde doorbreken van de beveiliging, is ondergebracht. In zoverre lijkt de onder 5.19. geciteerde passage uit de wetsgeschiedenis (deels) achterhaald.

5.21.

Wat naar mijn mening wel blijft staan, is, dat toegang moet worden verkregen tot dat andere onderdeel van de computer of tot die andere gegevens "op één van de strafbaar gestelde wijzen" alvorens sprake kan zijn van computervredebreuk als bedoeld in art. 138ab Sr.[29.] De volgende passage in de Memorie van Antwoord op pagina 32, hoewel ook weer multi-interpretabel, geeft mijns inziens steun aan deze opvatting:

"Het voorgestelde artikel 138a is, ook in zijn oorspronkelijke opzet, tevens van toepassing op het binnendringen in een gedeelte van een geautomatiseerd werk. Dit heeft niet alleen betrekking op bestanden met voor de mens leesbare informatie, maar ook op programma's. Iemand die is geautoriseerd tot de kennisneming van bepaalde bestanden, doch niet tot de wijziging daarvan, overtreedt dus de voorgestelde bepaling indien hij met overschrijding van zijn autorisatie binnendringt in de zin van dit artikel, in een gedeelte van het geautomatiseerd werk waar hij gebruik kan maken van de functie bestemd om de desbetreffende bestanden te wijzigen."

5.22.

Tot slot wijs ik op een passage uit de wetsgeschiedenis van de Wet Computercriminaliteit II, waarbij in de memorie van toelichting het volgende wordt gesteld:

"Artikel 138a Sr geeft primair bescherming aan (delen van) geautomatiseerde werken. De bescherming van de daarin aanwezige gegevens is daarvan een afgeleide. Daarbij maakt het niet uit om wat voor soort gegevens het gaat; (…). Onder «een deel» van een geautomatiseerd werk in de zin van artikel 138a Sr kan bijvoorbeeld worden verstaan de voor een bepaalde persoon gereserveerde ruimte op de harde schijf van een netwerkserver. Deze ruimte moet wel op een of andere wijze zijn afgeschermd (bijvoorbeeld door middel van een password), zodat onbevoegden haar niet zonder meer kunnen betreden. Hier wordt dus wel enige vorm van beveiliging van computergegevens (althans van de computer waarin zich die gegevens bevinden) geëist, in tegenstelling tot bijvoorbeeld de hiervoor besproken situatie dat gegevens over een telecommunicatienetwerk worden verzonden: (…)."[30.]

5.23.

Mijn tussenconclusie is dat uit de wetsgeschiedenis niet eenduidig kan worden opgemaakt of ook een *reglementaire* toegang tot een computersysteem, zonder dat daarvoor een beveiliging moet worden doorbroken, kan worden aangemerkt als binnendringen. De wetgever lijkt niet te hebben gedacht aan het oneigenlijk gebruiken van een eigen wachtwoord of een

verkregen autorisatie, zoals het hof heeft geoordeeld. Van de andere kant wordt in de wetsgeschiedenis wel gerept van de overschrijding van een autorisatie als het gaat om wederrechtelijk binnendringen. Op grond daarvan kan verdedigd worden dat onderhavige casus wel onder art. 138ab Sr valt te brengen. Alvorens ik deze vraag definitief beantwoord, ga ik eerst nader in op art. 138c Sr.

5.24.

Blijkens de wetsgeschiedenis is art. 138c Sr ingevoerd om het wederrechtelijk overnemen van gegevens, in algemene zin strafbaar te stellen. Daarbij hield de wetgever er rekening mee dat veel gevallen reeds onder andere strafbepalingen, waaronder art. 138ab Sr en art. 272 (schending van het ambtsgeheim), vallen. Art. 138c Sr is zogezegd een vangnetbepaling om gevallen te kunnen vervolgen waarbij er geen sprake is van wederrechtelijk binnendringen. Het overnemen van gegevens is alleen strafbaar voor zover dit wederrechtelijk is. Die wederrechtelijkheid "ontbreekt in het geval dat aangenomen mag worden dat de gegevens met toestemming van de rechthebbende zijn overgenomen. Als een medewerker in het kader van het thuiswerken gegevens uit een computer van het werk mee naar huis neemt op een usb-stick, is dit niet wederrechtelijk en daarmee niet op grond van (…) art. 138c Sr strafbaar als dit gebeurt met toestemming van de werkgever en/of voldoet aan door de werkgever gestelde regels."[31.] In de Memorie van Toelichting is als voorbeeld van het wederrechtelijk overnemen van gegevens het geval genoemd dat een overheidsmedewerker, die weliswaar rechtmatig toegang heeft tot bepaalde gegevens, deze vervolgens wederrechtelijk overneemt voor zichzelf of een ander. Op zichzelf zou het bewezenverklaarde in onderhavige zaak zonder twijfel zijn te brengen onder de strafbaarstelling van art. 138c Sr.

5.25.

Dan kom ik nu toe aan de doorslaggevende vraag of het hof heeft kunnen concluderen dat de verdachte in onderhavige zaak het computersysteem wederrechtelijk is binnengedrongen in de zin van art.138ab Sr door overschrijding van zijn autorisatie. Het hof beantwoordt deze vraag bevestigend omdat het volgens het hof vast staat dat de verdachte gebruik heeft gemaakt van een valse sleutel en een valse hoedanigheid.
Daarvoor is het op zichzelf, zoals hiervoor besproken, niet per se nodig dat dit gepaard gaat met het doorbreken van een beveiliging.

Valse hoedanigheid?

5.26.

Wat het aannemen van een valse hoedanigheid aangaat heb ik zo mijn twijfels. Hoewel het hof hierbij het juiste toetsingskader vooropstelt, vraag ik mij af of het hof voldoende inzichtelijk heeft gemaakt dat de verdachte daadwerkelijk een valse hoedanigheid heeft aangenomen bij het inloggen in Blue View. Volgens het door het hof aangehaalde arrest van de Hoge Raad van 20 december 2016[32.] over de "bonafide wederpartij", dienen in dat geval voldoende specifieke gedragingen te worden vastgesteld die in de desbetreffende context erop zijn gericht bij het beoogde slachtoffer (in casu de Politie) een onjuiste voorstelling van zaken in het leven te roepen teneinde daarvan misbruik te maken. Met de vaststelling dat de verdachte als politieambtenaar met zijn *eigen* accreditatie en inloggegevens inlogde op het systeem is het aannemen van een valse hoedanigheid nog niet gegeven. Onduidelijk blijft waarop het hof de aanname baseert dat de verdachte, door op deze wijze in te loggen, zich heeft *voorgedaan* als een onkreukbare politieambtenaar die (bevoegd) gegevens opvroeg in het kader van zijn politietaak. Uit welke specifieke gedragingen dit "voordoen" zou kunnen worden afgeleid, blijkt niet uit de bewijsmiddelen of de bewijsoverwegingen. Naar mijn mening is dan ook de bewezenverklaring dat de verdachte een valse hoedanigheid heeft aangenomen onvoldoende met redenen omkleed.

Valse sleutel?

5.27.

Dat zie ik anders waar het gaat om de vaststelling van het hof dat de verdachte gebruik heeft gemaakt van een valse sleutel. Zoals hiervoor is besproken wordt het begrip 'valse sleutel' door de Hoge Raad ruim uitgelegd en kan een sleutel, door het onbevoegd gebruikmaken daarvan een valse sleutel worden.

5.28.

In het onderhavige geval had de verdachte door middel van zijn accreditatie vrije toegang tot de gegevens. Hoewel het hof hier in zijn specifieke bewijsoverwegingen met betrekking tot feit 2 niet expliciet melding van heeft gemaakt, heeft het hof in zijn inleidende bewijsoverwegingen met betrekking tot feit 1, 2 en 3 (voorafgaand aan tussenconclusie 2) op het volgende gewezen:

"Op het eerste blad van elke export is een waarschuwing opgenomen voor de gebruiker:
'Het oneigenlijk gebruik dan wel misbruik van deze gegevens is ten strengste verboden. Daarnaast is het verstrekken van deze gegevens aan derden welke niet de vereiste autorisatie bezitten eveneens ten strengste verboden'.

De gebruiker kan pas verder gaan met exporteren als hij aangeeft dat hij de bovenstaande waarschuwing heeft gelezen en op OK drukt."[33.]

5.29.

Ik meen dan ook dat in de bewijsoverwegingen — in samenhang met elkaar bezien — besloten ligt, dat het hof heeft aangenomen dat de verdachte, door deze waarschuwing opzettelijk te negeren, zijn autorisatie heeft overschreden en dat door dit wederrechtelijk gebruik zijn autorisatie, "de eigen sleutel", als een valse sleutel kan worden aangemerkt. Voor dit oordeel van het hof is zowel in de hiervoor besproken jurisprudentie als in de wetsgeschiedenis van art. 138ab Sr steun te vinden. In de wetsgeschiedenis wordt immers gewag gemaakt van het 'overschrijden van de autorisatie' in welk geval er ook sprake kan zijn van binnendringen in (een gedeelte van) een geautomatiseerd werk. De eenvoud van de regel in de jurisprudentie dat (ook) het wederrechtelijk gebruik van een (eigen) sleutel, deze sleutel tot een valse sleutel maakt, spreekt in dat verband aan.

5.30.

Ik realiseer mij dat met deze uitleg de reikwijdte van het wederrechtelijk binnendringen zoals strafbaar gesteld in art. 138ab lid 1 Sr potentieel erg groot wordt. Immers een werknemer die uit nieuwsgierigheid grasduint in de voor hem met wachtwoord toegankelijke systemen zal dat (op basis van interne regels) al snel onbevoegd kunnen doen, omdat dit niet altijd (strikt) noodzakelijk is voor de functie-uitoefening. Ook indien de gegevens alleen worden bekeken en niet overgenomen zal reeds sprake zijn van het overtreden van het bepaalde in art. 138ab lid 1 Sr (het binnendringen). Complicerende factor daarbij is dat niet voor alle gevallen, zoals ook hier, reeds op voorhand en zonder nadere bewijsmiddelen ondubbelzinnig blijkt wanneer volgens de rechthebbende (in dit geval de politie) precies wel en niet sprake is van bevoegd gebruik van de gegeven accreditatie. Het spreekt voor zich dat sprake is van onbevoegd gebruik wanneer het gebruik tot doel heeft vertrouwelijke gegevens te openbaren aan onbevoegde derden, maar dient art. 138ab Sr ook van toepassing te zijn indien de gegevens slechts 'spontaan' maar zonder noodzaak voor de functie worden ingezien? Aan deze overpeinzingen kunnen naar mijn mening in dit geval voorbij worden gegaan omdat er in deze zaak geen sprake is van een grijs gebied. Uit de bewijsmiddelen blijkt immers overduidelijk dat de verdachte ten aanzien van de daarin met name genoemde personen al voorafgaande aan het inloggen in Blue View de intentie heeft gehad, in strijd met de in Blue View opgenomen waarschuwing, het systeem oneigenlijk te gebruiken. Daarmee heeft hij zijn autorisatie misbruikt, en dus het geautomatiseerd werk wederrechtelijk binnengedrongen (lid 1), en vervolgens ook in strijd met deze waarschuwing de hieruit verkregen gegevens aan onbevoegde derden verstrekt (lid 2).

5.31.

Ook al is naar mijn mening het aannemen van de valse hoedanigheid door de verdachte door het hof onvoldoende met redenen omkleed, heeft het hof mijns inziens wel kunnen aannemen dat de verdachte gebruik heeft gemaakt van een valse sleutel en door middel daarvan het geautomatiseerde systeem van Blue View wederrechtelijk is binnengedrongen. Ook met weglating van de passage die betrekking heeft op het aannemen van een valse hoedanigheid wordt de aard en de ernst van het bewezenverklaarde in zijn geheel beschouwd niet aangetast en ben ik van oordeel dat de bewezenverklaring voldoende conform de eis van de wet met redenen is omkleed.

5.32.

Het tweede middel is vergeefs voorgesteld.

Uitspraak

Hoge Raad:

2. Beoordeling van het tweede cassatiemiddel

2.1

Het cassatiemiddel klaagt onder meer over het oordeel van het hof dat de verdachte met behulp van een valse sleutel en door het aannemen van een valse hoedanigheid het politiesysteem Blue View wederrechtelijk is binnengedrongen.

2.2.1

Overeenkomstig de tenlastelegging onder 2 is ten laste van de verdachte bewezenverklaard dat:

"hij in de periode van 1 januari 2012 tot en met 29 september 2015 in Nederland telkens, opzettelijk en wederrechtelijk in een of meer (delen van) geautomatiseerde werken, namelijk in een of meer (delen van) servers van de politie en/of de belastingdienst, is binnengedrongen met behulp van een valse sleutel en door het aannemen van een valse hoedanigheid,

namelijk door onbevoegd gebruik te maken van een gebruikersnaam en wachtwoord (voor de applicatie Blue View) en door zich met een gebruikersnaam en wachtwoord (voor de applicatie Blue View) toegang te verschaffen tot (delen van de) servers van de politie (waarop de applicaties Blue View en/of BVH en/of BVO en/of Summ-it en/of FIU waren geplaatst) met een ander doel dan waarvoor hem die gebruikersnaam en dat wachtwoord ter beschikking stonden en waarvoor hem die toegang was toegestaan, en (vervolgens) gegevens die waren opgeslagen en verwerkt en overgedragen door middel van (delen van) die geautomatiseerde werk(en) waarin hij zich wederrechtelijk bevond, voor zichzelf en anderen heeft overgenomen, namelijk door (telkens) (vertrouwelijke) informatie (omtrent een of meer personen en opsporingsonderzoeken) uit de applicatie Blue View op (een) gegevensdrager(s) en/of in (een) document(en) te plaatsen en/of (naar zichzelf) te mailen en/of te exporteren en/of (vervolgens) aan daartoe niet-gerechtigde personen te verstrekken."

2.2.2

Het hof heeft ten aanzien van de bewezenverklaring onder meer overwogen:

"De loopbaan van verdachte bij de politie
Verdachte is op 26 januari 2009 aangesteld als aspirant in tijdelijke dienst gedurende de initiële opleiding (zes jaar) bij de Dienst Nationale Recherche (hierna: DNR). Hij is een zij-instromer op niveau 4. Op 21 november 2008 tekende verdachte daartoe een geheimhoudersverklaring van de Landelijke Eenheid en op 15 december 2008 werd een verklaring van geen bezwaar voor deze functie afgegeven. Op 22 april 2009 legde verdachte de ambtseed af en ondertekende hij het eedsformulier.
Op 13 juli 2010 werd verdachte aangesteld als generalist tactische recherche tot en met 31 juli 2011 en op 28 juli 2011 werd de proeftijd verlengd tot en met 31 januari 2012. Op 1 februari 2012 volgde een vaste aanstelling bij de DNR.
Op 14 oktober 2011 ontving het hoofd van het Bureau Veiligheid en Integriteit KLPD een brief 'Weigering verklaring van geen bezwaar' (hierna: VGB) met betrekking tot verdachte, waarin wordt vermeld dat verdachte van deze weigering op de hoogte is gesteld.
Door deze weigering kon verdachte niet bij de DNR blijven werken en werd hij op verschillende locaties tewerkgesteld. Hij werkte onder andere in 2013 bij de Dienst Verkeer van het KLPD in Driebergen in Maasbracht en in 2014 bij de Landelijk Eenheid, Dienst Infra, locatie Croeselaan te Utrecht. Daarnaast werkte hij nog in de regio Venlo en Eindhoven ten behoeve van het behalen van modules in het kader van zijn opleiding.
(…)
Blue View
Blue View is een indexsysteem, waarin dumps plaatsvinden van diverse politiesystemen, zoals BVO, Summ-it, HKS, BVH, Luris, FIU, afkomstig van bijna alle opsporingsinstanties van Nederland (Kmar, FIOD et cetera).
Accounts in Blue View zijn strikt persoonlijk en mogen niet gedeeld worden.
Om Blue View te raadplegen wordt ingelogd met een gebruikersnaam en een wachtwoord. De gebruikersnaam is het dienstnummer van de verbalisant, [001], zijnde verdachte. Hij had een Blue View account vanaf 29 augustus 2011 om 10.18 uur, op niveau Opsporing basis 3 en 4. Bevragingen geschieden op een zogenaamde lange KENO, een zoeksleutel gebaseerd op onder andere achternaam en geboortejaar van de te bevragen persoon. Resultaten van bevragingen kunnen worden geëxporteerd als PDF- of Excelbestand. Vervolgens kunnen deze worden opgeslagen op bijvoorbeeld een harde schijf van een computer of op een USB-stick, indien de gebruiker rechten heeft om gegevens op een USB-stick op te slaan. Verdachte had die rechten. In de naam die het document krijgt tijdens het exporteren zit de tekst 'Registratie Export'. Uit de bestandsnaam is af te leiden op welke datum de export is gemaakt en wat het accountnummer is van de gebruiker.
Op het eerste blad van elke export is een waarschuwing opgenomen voor de gebruiker:
'Het oneigenlijk gebruik dan wel misbruik van deze gegevens is ten strengste verboden. Daarnaast is het verstrekken van deze gegevens aan derden welke niet de vereiste autorisatie bezitten eveneens ten strengste verboden'. De gebruiker kan pas verder gaan met exporteren als hij aangeeft dat hij de bovenstaande waarschuwing heeft gelezen en op OK drukt.
(…)
Voorts is door de verdediging aangevoerd dat de 28.521 logregels in Blue View niet representatief zijn voor het aantal zoekopdrachten, nu elke mutatie in Blue View een nieuwe logregel creëert. Verdachte schat zelf dat hij ongeveer 5000 bevragingen heeft uitgevoerd. Ter onderbouwing van dit verweer heeft de verdediging het navolgende naar voren gebracht.

a. Verdachte heeft bij de rechter-commissaris en ter zitting in eerste aanleg en hoger beroep aangevoerd dat niet kan worden aangenomen dat alle bevragingen in die periode illegaal werden gedaan. Hij werd immers, ook nadat hij niet meer bij de DNR werkzaam was, juist speciaal in onderzoeken ingezet met de vraag om gebruik te maken van zijn accreditatie voor Blue View en ook omdat hij een zekere handigheid had in het bevragen van dat systeem.

b. (…)

Het hof overweegt, samen met de rechtbank, met betrekking tot deze stellingen van verdachte het volgende:

a. Dat verdachte wel eens door collega's zou zijn benaderd om Blue View te bevragen wordt ook door de getuigen [betrokkene 2] en [betrokkene 3] bij de rechter-commissaris niet ontkend, zij het dat zij hem zelf nooit gevraagd hebben Blue View te raadplegen. Het hof sluit dan ook niet uit dat het heel wel kan zijn dat verdachte op verzoek

wel eens ten behoeve van opsporingsonderzoeken Blue View heeft bevraagd, ook nadat hij niet meer bij de DNR werkzaam was. Hij had immers zijn accreditatie op niveau 3 en 4 gewoon behouden. Gelet op de enorme hoeveelheid gevoelige informatie die door verdachte is bevraagd, welke niet allemaal volledig is onderzocht, is het niet uit te sluiten dat verdachte op verzoek van collega's daadwerkelijk wel eens informatie uit het systeem heeft opgevraagd. Door verdachte is overigens geen enkel voorbeeld aangewezen waarbij dat het geval zou zijn geweest. Het hof is echter van oordeel, dat dit onverlet laat dat door verdachte zonder enige professionele aanleiding of intern verzoek ook grote hoeveelheden vertrouwelijke informatie zijn bevraagd en geëxporteerd die aangetroffen zijn bij derden zoals het hof hierna nog zal bespreken. Wat er ook zij van het verweer, het staat een bewezenverklaring niet in de weg. Het verweer faalt daarom reeds in zoverre.

(…)

Met betrekking tot feit 2: computervredebreuk

De advocaat-generaal stelt zich op het standpunt dat dit feit bewezen kan worden verklaard.

Door de verdediging is vrijspraak bepleit. Daartoe heeft zij — kort gezegd — het volgende aangevoerd. Er is geen sprake van het zogenaamd ‘hacken’ zoals bedoeld in artikel 138ab Wetboek van Strafrecht. De rechtbank heeft het begrip ‘binnendringen’ verkeerd uitgelegd. Dit artikel strekt namelijk niet tot de bescherming van de (inhoud van) gegevens, maar is bedoeld om het binnendringen op zich strafbaar te stellen. Dit blijkt des te meer uit het nieuwe artikel 138c Wetboek van Strafrecht, in welk artikel het met rechtmatig toegang wederrechtelijk overnemen van gegevens strafbaar is gesteld. Van dergelijk binnendringen is thans geen sprake, nu verdachte beschikte over een rechtmatige 'sleutel', te weten zijn accreditatie om Blue View te raadplegen. Bovendien is geen sprake van een valse hoedanigheid, doorbreken van beveiliging of technische ingreep van de zijde van verdachte, aldus de verdediging.

Het hof stelt, onder verwijzing naar artikel 80sexies Sr zoals geldend ten tijde van het tenlastegelegde, samen met de rechtbank vast dat — zoals bij de bespreking van feit 1 aan de orde is geweest — het Blue View systeem een geautomatiseerd werk is, in casu zijnde een digitaal verzamelsysteem dat door politieambtenaren in de uitoefening van hun politietaak kan worden geraadpleegd mits zij daarvoor zijn geaccrediteerd en beschikken over een autorisatie. Er moeten om in het beveiligde systeem te komen een gebruikersnaam (dienstnummer) en wachtwoord worden gegeven. Verdachte beschikte over een zodanige autorisatie vanaf 29 augustus 2011 tot zijn aanhouding op 29 september 2015.

Het hof overweegt omtrent het verweer dat verdachte rechtmatig beschikte over een autorisatie waarmee hij Blue View kon raadplegen en dat daarmee geen veroordeling ter zake van het onder 2 tenlastegelegde kan volgen, als volgt.

(…)

Het schenden van artikel 138ab Sr was tot de inwerkingtreding van de Wet kraken en leegstand (*Stb.* 2010, 320) tot 1 oktober 2010 geregeld in art. 138a Sr. Op grond van de parlementaire stukken kan ter zake van het huidige art. 138ab Sr — het toenmalige art. 138a Sr — het volgende worden opgemerkt.

De strafbaarstelling van art. 138ab Sr beschermt degene die blijkens feitelijke beveiliging heeft duidelijk gemaakt dat hij zijn gegevens heeft willen afschermen tegen nieuwsgierige blikken door het systeem daartegen te beveiligen. De bescherming van gerechtvaardigde belangen van houders van gegevensbestanden die, opgeslagen in computers, vooral via de telecommunicatie-infrastructuur voor onbevoegde blikken toegankelijk zijn, wordt via deze strafbaarstelling geboden doordat het doorbreken van een aangebrachte beveiliging wordt strafbaar gesteld. Daarbij is aansluiting gezocht bij de bestaande strafbaarstelling betreffende de huisvredebreuk. De eisen rondom wederrechtelijke binnendringing zijn in de sfeer van de informatietechniek in deze strafbaarstelling vertaald in het bestanddeel ‘binnendringen’, inhoudende dat een beveiliging moet zijn doorbroken. In de Memorie van Toelichting is hierover opgenomen: ‘Het gaat er om dat degeen die de computer binnendringt door het doorbreken van de beveiliging, heeft blijk gegeven de wetenschap te hebben gehad dat hij een beveiligd systeem binnendringt en doelbewust enige inspanning heeft gedaan de beveiliging te doorbreken’ (vgl. *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 16).

Het aangehaalde lid 1 van artikel 138ab Sr geeft aan dat van ‘binnendringen’ in ieder geval sprake is indien de toegang tot het werk wordt verworven met behulp van een valse sleutel of door het aannemen van een valse hoedanigheid. In de Kamerstukken van het toenmalige wetsvoorstel wordt over het bestanddeel ‘valse sleutel’ weergegeven dat een password een sleutel is die de gebruiker toegang geeft tot het systeem of tot een deel daarvan. Daarbij werd aangehaald dat de Hoge Raad in zijn arrest van 20 mei 1986, ECLI:NL:HR:1986:AC9359, *NJ* 1987/130, heeft bepaald dat een huissleutel die wordt gebruikt tot opening van een slot door iemand die daartoe niet is gerechtigd, een valse sleutel is en dat niet is vereist dat ten aanzien van de sleutel enige beveiligingsmaatregel is genomen. Onder verwijzing naar artikel 90 Sr, waarin geen definitie van het begrip ‘valse sleutels’ wordt gegeven maar enkel wordt aangegeven wat onder het begrip dient te worden begrepen (‘alle tot opening van het slot niet bestemde werktuigen’) — waarbij de wetgever heeft aangegeven dat '(O)nverschillig (is) of het werktuig al of niet een sleutel is, zoo het slechts niet die sleutel is, die voor opening van dat slot bestemd is.' (zie H.J. Smidt, *Geschiedenis van het Wetboek van Strafrecht*, Deel I, tweede druk, p. 544) — stelt het hof dat de jurisprudentie van de Hoge Raad verder ter zake van ‘valse sleutel’ heeft uitgemaakt dat ook onrechtmatig gebruik van bijvoorbeeld een bankpas of een tankpas kan worden aangemerkt als het gebruik maken van een ‘valse sleutel’. Anders gezegd: de Hoge Raad geeft een ruime uitleg aan het begrip ‘valse sleutels’ waarbij ook gebruik door een onbevoegde als een ‘valse sleutel’ kan worden aangemerkt (vgl. CAG Knigge in ECLI:NL:PHR:2017:1012 onder verwijzing naar HR 3 oktober 2017,

ECLI:NL:HR:2017:2546).
Voor wat betreft de uitleg in de genoemde bepaling ter zake van het bestanddeel ‘valse hoedanigheid’ wijst het hof op de uitleg die de Hoge Raad daaraan geeft in zijn overzichtsarrest van 20 december 2016, ECLI:NL:HR:2016:2892, *NJ* 2017/158, m.nt. Keijzer, rov. 2.3.4. De Hoge Raad heeft ter zake van het aannemen van een valse hoedanigheid overwogen dat het daarbij in de kern erom gaat dat het handelen van de verdachte ertoe kan leiden dat bij de ander een onjuiste voorstelling van zaken in het leven wordt geroepen met betrekking tot de 'persoon' van de verdachte wat betreft diens hoedanigheid, waarbij die onjuiste voorstelling van zaken in het leven wordt geroepen teneinde daarvan misbruik te maken. Daarbij heeft de Hoge Raad specifiek aangegeven dat de in de rechtspraak wel gebruikte formulering dat een verdachte zich als een 'bonafide' deelnemer aan het rechtsverkeer heeft gepresenteerd, met betrekking tot het aannemen van een valse hoedanigheid slechts relevant is als zo een presentatie als bonafide (potentiële) wederpartij berust op voldoende specifieke gedragingen die in de desbetreffende context erop zijn gericht bij het beoogde slachtoffer een onjuiste voorstelling van zaken in het leven te roepen teneinde daarvan misbruik te maken.
De verdachte heeft op enig moment, namelijk toen hij werkzaam zou worden bij de Nationale Recherche toegang gekregen tot het beveiligde Blue View systeem. Om Blue View te kunnen raadplegen, heeft verdachte moeten inloggen met een gebruikersnaam (zijn dienstnummer) en een wachtwoord. Daarmee verkreeg verdachte ook de bevoegdheid om de resultaten van bevragingen te kunnen exporteren als PDF of Excel-bestand en op te slaan op bijvoorbeeld een externe opslagplaats, zoals een USB stick. Verdachte werd daarbij uitdrukkelijk via het systeem gewaarschuwd dat oneigenlijk gebruik dan wel misbruik van deze gegevens, waaronder het verstrekken van deze gegevens aan derden welke niet de vereiste autorisatie bezitten, ten strengste verboden was. Zoals hierboven weergegeven zijn deze werkzaamheden spoedig gestaakt omdat hij geen 'Verklaring van geen bezwaar' verkreeg. Desalniettemin heeft verdachte nog jaren dit systeem ingezien.
Het hof oordeelt dat verdachte op grond van de in het voorgaande weergegeven feiten en omstandigheden het beveiligde politiesysteem Blue View, dat hij in het kader van zijn specifieke werkzaamheden als politieambtenaar op die betreffende gegevens niet behoefde en niet behoorde in te zien, heeft misbruikt om informatie/gegevens over criminelen in te zien, deze informatie/gegevens over te nemen en deze informatie/gegevens ook aan deze criminelen te verstrekken. Hij is met behulp van de aan hem toegekende autorisatie het systeem Blue View opzettelijk en wederrechtelijk binnengedrongen om inzage te krijgen van gegevens waar hij niet toe bevoegd was en vervolgens deze over te nemen. Door op deze wijze de betreffende gegevens in te zien en over te nemen, heeft verdachte, wetende dat het een beveiligd systeem betrof, doelbewust de beveiliging van dit systeem doorbroken en is hij derhalve het systeem binnengedrongen. Hij heeft zich daarbij bediend van een valse sleutel en het aannemen van een valse hoedanigheid. Verdachte heeft immers weliswaar geautoriseerd maar onbevoegd ter zake van de betreffende gegevens zich opzettelijk en wederrechtelijk de toegang verschaft tot het systeem Blue View. Daarbij was aan verdachte de autorisatie verstrekt om het systeem te raadplegen om in het kader van zijn werk als politieambtenaar naspeuringen te verrichten, maar niet om daarmee informatie in te winnen en dit aan criminelen te verstrekken waardoor dezen zich aan die naspeuringen konden onttrekken. Tevens heeft verdachte in de context van zijn handelen als politieambtenaar voldoende specifieke gedragingen verricht om een onjuiste voorstelling van zaken in het leven te roepen met betrekking tot de hoedanigheid van de 'persoon' van de verdachte. Verdachte heeft namelijk onder de voorstelling van de hoedanigheid van een persoon die gerechtigd was om op grond van zijn werkzaamheden inzage in de betreffende gegevens te mogen verrichten, zich de toegang verschaft tot het systeem Blue View, teneinde daarvan misbruik te maken. Verdachte bevroeg vele personen in het Blue View systeem zonder dat is gebleken dat daartoe in de uitoefening van zijn politietaak enige aanleiding bestond. Zowel de collega’s van verdachte als de maatschappij mocht erop vertrouwen — mede gelet op de aard en de functie van verdachte en de ambtseed die hij heeft moeten afleggen — dat zij te maken hadden met een betrouwbare en onkreukbare ambtenaar. Verdachte heeft echter op bedrieglijke wijze misbruik gemaakt van het vertrouwen van en in de politie.
Anders dan de verdediging is het hof van mening dat de strafbaarstelling opgenomen in artikel 138c Sr geen inbreuk maakt op een mogelijke bewezenverklaring van hetgeen aan verdachte onder 2 is tenlastegelegd en strafbaar is gesteld onder artikel 138ab Sr. De wetgever heeft in artikel 138c Sr strafbaar gesteld het opzettelijk en wederrechtelijk voor zichzelf of voor een ander overnemen van niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk. De bepaling is vooral van belang voor gevallen waarin de dader rechtmatige toegang heeft tot de gegevens, maar deze wederrechtelijk overneemt (vgl. *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 64). In de onderhavige zaak had verdachte weliswaar autorisatie om toegang te krijgen tot het systeem Blue View, maar hij was niet bevoegd tot het inzien en overnemen van de gegevens waar het in de onderhavige strafzaak om gaat. Verdachte heeft derhalve met behulp van de aan hem toegekende autorisatie het systeem Blue View opzettelijk en wederrechtelijk binnengedrongen om inzage te krijgen van gegevens waar hij niet toe bevoegd was en vervolgens deze overgenomen.
Het hof is dan ook van oordeel dat de tenlastegelegde computervredebreuk bewezen kan worden verklaard.”

2.3.1

De tenlastelegging is toegesneden op artikel 138ab van het Wetboek van Strafrecht (hierna: Sr). Daarom moet worden aangenomen dat de in de tenlastelegging en de bewezenverklaring voorkomende begrippen “wederrechtelijk

binnengedrongen", "valse sleutel" en "valse hoedanigheid" zijn gebruikt in de betekenis die deze begrippen hebben in die bepaling.

2.3.2

Artikel 138ab lid 1 en 2 Sr zoals dat gold vanaf 1 oktober 2010 — en dat op het aan de orde zijnde punt niet verschilt van de nu geldende tekst — luidde:

"1. Met gevangenisstraf (…) wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:

a. door het doorbreken van een beveiliging,

b. door een technische ingreep,

c. met behulp van valse signalen of een valse sleutel, ofd. door het aannemen van een valse hoedanigheid.

2. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt."

2.3.3

De strafbaarstelling van computervredebreuk was tot 1 oktober 2010 opgenomen in artikel 138a (oud) Sr. Deze bepaling is ingevoerd bij Wet van 23 december 1992 tot wijziging van het Wetboek van Strafrecht en van het Wetboek van Strafvordering in verband met de voortschrijdende toepassing van informatietechniek (Wet computercriminaliteit), *Stb.* 1993, 93. Volgens de memorie van toelichting geeft het wetsvoorstel uitvoering aan het rapport 'Informatietechniek en strafrecht' van de Commissie computercriminaliteit (Commissie Franken). In dat rapport is ten aanzien van de voorgestelde strafbaarstelling van computervredebreuk onder meer het volgende vermeld (p. 59-60):

"98 (…) Van 'binnendringen' is sprake (zo is althans de opvatting ten aanzien van de term in artikel 138 Sr) indien men zich de toegang verschaft tegen de onmiskenbare wil van de rechthebbende, welke zowel uit woorden als daden kan blijken. In het eerste geval zou voor strafbaarheid van het pogen de toegang te verkrijgen tot informatietechnische systemen een tekst 'verboden toegang voor onbevoegden' volstaan (maar: zie 100). In het tweede geval zou een duidelijke drempel moeten bestaan zodat onbevoegden zich niet simpelweg toegang kunnen verschaffen. Men denke hier aan wachtwoorden, PIN-codes en dergelijke: indien gebruik daarvan nodig is om toegang te krijgen, openbaart zich daarmee de wil van de rechthebbenden onbevoegden de toegang te weigeren.

99 Een inperking geeft de toevoeging van de term 'wederrechtelijk'. Of zich wederrechtelijkheid voordoet, zou moeten worden vastgesteld in het licht van de verhouding tussen degene die binnendringt en degene in wiens systeem wordt binnengedrongen. Daarbij speelt een rol of er duidelijke afspraken zijn, en of sprake is van (ongeschreven) regels in het maatschappelijk verkeer.

Zo kan men zich afvragen of van wederrechtelijk binnendringen bijvoorbeeld ook sprake is wanneer een persoon die werkzaam is in een bedrijf of instelling en aan wie door de leiding de bevoegdheid is gegeven om alleen bestaande delen van het gegevensverwerkend systeem te benaderen, binnendringt in andere niet voor hem opengestelde delen. De commissie meent dat de jurisprudentie rond het bestanddeel 'wederrechtelijk binnendringen' in artikel 138 Sr leert dat deze term ook in dit verband in zich voordoende gevallen een voldoende onderscheidend vermogen zal hebben om te bepalen wat wel en wat niet als strafbaar moet worden aangemerkt. Tevens leert die jurisprudentie betreffende artikel 138 Sr dat de praktijk dermate verscheiden is dat het a priori pogen te vinden van nadere criteria waarschijnlijk een onbevredigend resultaat geeft — een dergelijke verscheidenheid zal immers ook bij computervredebreuk aanwezig zijn.

Duidelijk is wel dat de 'hacker', die van buitenaf (dat wil zeggen via de openbare telecommunicatie-infrastructuur) beveiligde systemen binnendringt zonder meer onder de werking van de voorgestelde bepaling zal vallen.

100 Met betrekking tot de zinsnede 'een daartegen beveiligd werk' wordt het volgende opgemerkt. In alinea 98 is betoogd dat van binnendringen sprake is, indien men zich toegang verschaft tegen de onmiskenbare wil van de rechthebbende — deze wil zou kunnen blijken uit woorden ('verboden toegang') of uit daden. De commissie meent dat woorden alleen niet voldoende zijn. Woorden, bijvoorbeeld de tekst op het beeldscherm dat toegang voor onbevoegden verboden is, geven wel onmiskenbaar een wil van de rechthebbende weer, doch sluiten toegang per ongeluk niet uit. Dit gevaar is in veel mindere mate aanwezig bij een hogere drempel, bestaande uit bepaalde, tegen het wederrechtelijk binnendringen gerichte, beveiligingsmaatregelen. Hiermee is een nadere inperking aangebracht. De deur moet als het ware niet alleen dicht zijn, maar ook op slot.

101 In het tweede lid staat een — niet limitatieve — opsomming van manieren waarop onbevoegd toegang kan zijn verkregen, wil van binnendringen sprake zijn. De formulering is zo dat diverse manieren om toegangsbeveiligingen te doorbreken, dan wel te omzeilen, er onder te brengen zijn.

Gesproken wordt van een 'valse hoedanigheid', 'listige kunstgrepen' (conform artikel 326 Sr) en van een 'valse sleutel' (conform artikel 90 Sr). De commissie beoogt daarmee die situaties onder de werking van de strafbepaling te brengen, waarin men de beschikking heeft verkregen over overigens geldige toegangsmiddelen, echter zonder toestemming van de

beheerder van de inrichting of de houder van de toegangsmiddelen.
(…)
De termen ‘valse hoedanigheid’ en ‘valse sleutel’ zien op het gebruik van niet legaal verkregen toegangsmiddelen. Degene die een magneetpas of een toegangscode van een ander zonder diens toestemming gebruikt, hult zich in de valse hoedanigheid van de bevoegde gebruiker of maakt gebruik van een valse sleutel, wanneer de toegangsprocedure niet in een identificatie doch slechts in een autorisatie van de gebruiker voorziet.”

2.3.4

De memorie van antwoord aan de Tweede Kamer bij het wetsvoorstel dat heeft geleid tot de Wet computercriminaliteit houdt ten aanzien van het voorgestelde artikel 138a Sr onder meer het volgende in:

“Ingevolge de nieuw in de nota van wijziging voorgestelde bepaling is al sprake van strafbaarheid indien de toegang is verkregen door listige kunstgrepen, een valse sleutel of het aannemen van een valse hoedanigheid. Ik ga er daarbij vanuit dat een password een sleutel is die de gebruiker toegang geeft tot het systeem of tot een deel daarvan.” (*Kamerstukken II* 1990/91, 21551, nr. 6, p. 31)

2.4.1

Het hof heeft vastgesteld, kort gezegd, dat de verdachte als politieambtenaar voorafgaand aan de bewezenverklaarde periode een autorisatie heeft verkregen voor toegang tot het beveiligde politiesysteem Blue View, waartoe hij de beschikking had over een gebruikersnaam (zijn dienstnummer) en een wachtwoord. Verder heeft het hof vastgesteld dat die autorisatie aan de verdachte was verstrekt om in het kader van zijn werk als politieambtenaar naspeuringen te verrichten, maar dat de verdachte het systeem vervolgens heeft bevraagd op gegevens over personen zonder dat daarvoor in de uitoefening van zijn politietaak enige aanleiding bestond. Op die manier kreeg de verdachte zonder daartoe bevoegd te zijn inzage in gegevens en nam hij deze gegevens over. Op grond hiervan heeft het hof geoordeeld dat de verdachte zijn autorisatie voor toegang tot het systeem Blue View heeft “misbruikt om informatie/gegevens over criminelen in te zien, deze informatie/gegevens over te nemen en deze informatie/gegevens ook aan deze criminelen te verstrekken”.

2.4.2

Het op dit misbruik van die autorisatie gebaseerde oordeel van het hof dat de verdachte met behulp van een “valse sleutel” als bedoeld in artikel 138ab lid 1, onder c, Sr een (deel van een) geautomatiseerd werk wederrechtelijk is binnengedrongen, geeft mede in het licht van de onder 2.3.3 en 2.3.4 weergegeven totstandkomingsgeschiedenis van (het huidige) artikel 138ab Sr niet blijk van een onjuiste rechtsopvatting. Dat oordeel is ook niet onbegrijpelijk.

2.4.3

Het oordeel van het hof dat de verdachte aldus ook door het aannemen van een “valse hoedanigheid” als bedoeld in artikel 138ab lid 1, onder d, Sr een (deel van een) geautomatiseerd werk wederrechtelijk is binnengedrongen, kan echter niet zonder meer uit de bewijsvoering worden afgeleid. De door het hof in aanmerking genomen omstandigheid dat de verdachte met het misbruik van zijn autorisatie het door zijn collega’s en de maatschappij in hem gestelde vertrouwen heeft geschonden, volstaat daartoe niet. De Hoge Raad neemt daarbij in aanmerking dat niet blijkt dat de verdachte al een valse hoedanigheid had aangenomen toen hem de autorisatie werd verstrekt. Het slagen van de hierop gerichte klacht leidt echter, mede gelet op wat onder 2.4.2 is overwogen, niet tot cassatie omdat het weglaten van dit deel van de bewezenverklaring de aard en de ernst van het bewezenverklaarde in zijn geheel beschouwd niet aantast.

2.5

Het cassatiemiddel is tevergeefs voorgesteld.

(…)

4. Ambtshalve beoordeling van de uitspraak van het hof

De verdachte bevindt zich in voorlopige hechtenis. De Hoge Raad doet uitspraak nadat meer dan zestien maanden zijn verstreken na het instellen van het cassatieberoep. Dat brengt mee dat de redelijke termijn als bedoeld in artikel 6 lid 1 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden is overschreden. Dit moet leiden tot vermindering van de opgelegde gevangenisstraf van vijf jaren.

5. Beslissing

De Hoge Raad:

- vernietigt de uitspraak van het hof, maar uitsluitend wat betreft de duur van de opgelegde gevangenisstraf;
- vermindert deze in die zin dat deze vier jaren en tien maanden beloopt;
- verwerpt het beroep voor het overige.

Noot

Auteur: J.M. ten Voorde

1.

Art. 138ab lid 1 Sr stelt strafbaar het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of een deel daarvan. Ietwat ongebruikelijk (nogal eens is er een ander lid in een artikel voor gereserveerd, zie onder andere art. 140 lid 4 en art. 151b lid 3 Sr) wordt in het eerste lid ook aangegeven wat in ieder geval onder binnendringen wordt verstaan. Het komt daarbij in de kern neer op het zich verwerven van toegang tot (een deel van) een geautomatiseerd werk. Dat kan op uiteenlopende manieren geschieden. De wet geeft een niet-limitatieve lijst van voorbeelden (in lid 1 genummerd a tot en met d): door het doorbreken van een beveiliging of een technische ingreep, met behulp van valse signalen of een valse sleutel of door het aannemen van een valse hoedanigheid.
De vraag die bij de strafbaarstelling van computervredebreuk een punt van discussie is, is in hoeverre voor binnendringen is vereist dat het geautomatiseerd werk is beveiligd. De geschiedenis van art. 138ab Sr is er één van relativering van de eis van beveiliging. De advocaat-generaal wijst daarop in haar conclusie (punt 5.20). Van het wegvallen van deze eis is evenwel geen sprake. Het lijkt juister om te zeggen dat beveiliging thans op verschillende wijzen kan worden begrepen. Dat heeft gevolgen voor de betekenis die aan binnendringen kan worden gegeven. Binnendringen kan geschieden door het doorbreken van een beveiliging. In dat geval zou je kunnen stellen dat met binnendringen de beveiliging (geheel of ten dele) stuk gaat. Ook binnendringen met een technische ingreep kan plaatsvinden door het stuk maken van (een deel van) een beveiliging. Deze wijzen van binnendringen sluiten aan bij de klassieke omschrijving van binnendringen in art. 138a (oud) Sr als het doorbreken van de beveiliging, waarvan de dader wetenschap heeft gehad en doelbewust enige inspanning heeft gedaan de beveiliging te doorbreken (*Kamerstukken II* 1989/90, 21551, nr. 3, p. 16). Met handelingen als het gebruik maken van valse signalen of een valse sleutel of door het aannemen van een valse hoedanigheid hoeft bij binnendringen niets stuk te gaan. Er is in die gevallen sprake van het omzeilen of het misleiden of bedriegen van een aangebrachte beveiliging. Hier gaat de beveiliging niet stuk; zij blijft intact. De dader heeft slechts een manier gevonden om de beveiliging te passeren.

2.

Met het aanbrengen van een beveiliging geeft de rechthebbende aan ten aanzien van (een deel van) een geautomatiseerd werk de toegang ertoe te willen beperken. De mate van beperking zal van de wil van de rechthebbende afhangen. Hij kan bepalen dat anderen dan hijzelf zich toegang mogen verwerven tot (een deel van) zijn geautomatiseerd werk. Zij worden daartoe geautoriseerd. Ook aan het toegang verwerven kan de rechthebbende voorwaarden verbinden. Een eis kan zijn dat slechts toegang kan worden verworven wanneer gebruik wordt gemaakt van een door de rechthebbende verstrekte gebruikersnaam en een door de gebruiker te bedenken wachtwoord dat eventueel aan door de rechthebbende gestelde voorwaarden moet voldoen. Gebruikersnaam en wachtwoord zijn meestal hoogstpersoonlijk en mogen niet aan derden worden verstrekt, laat staan door hen worden gebruikt. Het onbevoegde gebruik ervan door een derde levert wederrechtelijk binnendringen met behulp van een valse sleutel op en is strafbaar op grond van art. 138ab Sr. Met onbevoegd kan worden bedoeld zonder toestemming van de houder van de gebruikersnaam en het wachtwoord en/of zonder (expliciete) toestemming van de rechthebbende van (een deel van) het geautomatiseerde werk.
Het laatste geval laat zich in tenminste twee varianten denken. Toegang kan worden verworven door een derde persoon die gebruik maakt van de gebruikersnaam en wachtwoord van een houder. Die houder kan ze hebben verstrekt, zonder daartoe bevoegd te zijn geweest of ze zijn zonder bewust handelen van de houder in handen gekomen van een derde. Toegang kan ook worden verworven door de houder van de gebruikersnaam en het wachtwoord. In de regel levert dat geen computervredebreuk op. Daarop zijn uitzonderingen te bedenken. De vraag die in het onderhavige arrest centraal stond was of er sprake is van wederrechtelijk binnendringen met behulp van een valse sleutel door als houder met eigen gebruikersnaam en wachtwoord toegang te verwerven tot een geautomatiseerd werk, terwijl hij in de gegeven omstandigheden daartoe niet bevoegd was. Deze vraag was nog niet eerder aan de Hoge Raad voorgelegd. Advocaat-generaal Spronken laat in haar conclusie zien dat de parlementaire geschiedenis van de strafbaarstelling van computervredebreuk op dit punt aan duidelijkheid te wensen overlaat. Toch ziet zij voldoende redenen het veroordelend arrest van het hof in stand te laten. Ook de Hoge Raad verwerpt het cassatieberoep voor zover het gaat om wederrechtelijk binnendringen met een valse sleutel.

3.

Alvorens op het oordeel van de Hoge Raad in te gaan, lijkt het goed de feiten te belichten en ze in perspectief te plaatsen. Verdachte was ten tijde van de bewezenverklaarde feiten werkzaam als politieambtenaar. De bewezenverklaarde feiten houden in dat hij zich toegang heeft verworven tot politiegegevens. Het kennis nemen (als onderdeel van verwerken) daarvan door politieambtenaren is geregeld in de Wet Politiegegevens (Wpg). Politieambtenaren mogen politiegegevens

slechts verwerken in het kader van de uitvoering van de politietaak als bedoeld in art. 3 en 4 Politiewet 2021 (art. 6 lid 2 jo. 1, onder a Wpg). Zij mogen slechts worden verwerkt door politieambtenaren die zijn belast met de genoemde politietaak en die daartoe expliciet zijn geautoriseerd en voor zover hun autorisatie strekt. De autorisatie 'bevat een duidelijke omschrijving van de verwerkingen waartoe de betreffende ambtenaar wordt geautoriseerd en de onderdelen van de politietaak ter uitvoering waarvan de verwerkingen worden gedaan' (art. 6 lid 3 Wpg). Ook verdachte was tot het verwerken van politiegegevens geautoriseerd. Hij had om die reden toegang tot onder meer Blue View, een verzamelbox van politiegegevens. Verdachte was een fervent gebruiker van Blue View. Hij zocht niet alleen zeer frequent naar gegevens, hij downloadde ze ook en stelde ze ter beschikking aan derden. Politieambtenaren zijn met betrekking tot door hen verwerkte gegevens echter tot geheimhouding verplicht (art. 7 Wpg). Een niet onbelangrijk deel van de door verdachte verwerkte gegevens had betrekking op personen die met de verkregen informatie uit handen van de politie trachtten te blijven. Verdachte traineerde dus verschillende opsporingsonderzoeken. Dat deed hij gedurende langere periode. De vraag komt op hoe dat mogelijk is, vooral omdat toezicht moet worden uitgeoefend op aan politieambtenaren verstrekte autorisaties en autorisatieniveaus. Over het uitoefenen van toezicht is in het algemeen evenwel veel te doen geweest. De politie had haar zaakjes op dit punt lange tijd niet op orde (Inspectie Justitie en Veiligheid, *Maatregelen integriteit*, Den Haag 2016; Politie, *Interne audit Wpg derde cyclus* 2015-2018, 2019). Het lijkt in het onderhavige geval een kwestie te zijn geweest van: de gelegenheid schept de hacker. Die gelegenheid maakt overigens nog niet dat de hacker dus een valse hoedanigheid heeft aangewend, zoals het hof in casu vaststelde. Dat ligt volgens de Hoge Raad anders wanneer de politieambtenaar reeds vanaf het moment dat hij tot het verwerken van politiegegevens was geautoriseerd die gegevens om andere redenen wilde verwerken dan in het kader van de uitvoering van zijn politietaak (r.o. 2.4.3).

4.

Het uitstapje naar de Wpg leert dat politieambtenaren zich toegang mogen verwerven tot een (deel van een) geautomatiseerd werk in het kader van het verwerken van politiegegevens. Daarbij geldt dat zij deze slechts mogen verwerken in het kader van de uitvoering van de politietaak en voor zover zij tot het verwerken ervan zijn geautoriseerd. Aan die autorisatie wordt in het cassatiemiddel enige waarde gehecht. Verdachte werkte enige tijd bij de Dienst Nationale Recherche van het toenmalige Korps Landelijke Politiediensten. Hij kreeg ten behoeve van zijn werkzaamheden aldaar een autorisatie van een bepaald niveau. Na weigering van een Verklaring van geen bezwaar werd hij elders te werk gesteld. Hij behield echter zijn autorisatie, vermoedelijk ten onrechte. Of dat zo is, laat het hof in het midden. Dat kon het hof ook doen omdat het al of niet ten onrechte hebben gehad van een autorisatie ten tijde van het bewezenverklaarde feiten niet in de weg staat aan het oordeel dat verdachte met behulp van een valse sleutel wederrechtelijk is binnengedrongen. Ervan uitgaande dat verdachte was geautoriseerd om in te loggen in Blue View, mocht hij slechts daarop naspeuringen verrichten 'in het kader van zijn werk als politieambtenaar'. Om andere redenen inloggen in Blue View ('zonder enige professionele aanleiding', zoals het hof het formuleert) was verdachte niet toegestaan. Maar het is precies dat wat verdachte deed. Ik meen dat dit de conclusie rechtvaardigt dat verdachte met behulp van een valse sleutel wederrechtelijk is binnengedrongen in een geautomatiseerd werk. Hoewel hij gebruik maakte van zijn eigen sleutel (bestaande uit een gebruikersnaam en wachtwoord), hij geautoriseerd was om met die sleutel toegang te verwerven tot Blue View, mocht hij niet inloggen op Blue View om een andere reden dan in het kader van de uitoefening van zijn politietaak. Nu hij dat wel (en veelvuldig) deed, is er sprake van wederrechtelijk binnendringen met behulp van een valse sleutel. Voor het bewijzen van binnendringen komt het er dan wel op aan vast te stellen of verdachte ten tijde van de ten laste gelegde periode inlogde op Blue View met een andere reden (of doel) dan in het kader van het uitoefenen van de politietaak. Daarbij lijkt irrelevant of hij soms wel in dat kader inlogde, indien is vastgesteld dat hij ook om andere redenen inlogde dan in het kader van zijn taakuitoefening.
Het hof, de advocaat-generaal en de Hoge Raad richten hun pijlen niet alleen of zelfs niet zozeer op het binnendringen in de zin van het toegang verwerven. Zij richten zich vooral op verdachtes gedragingen nadat hij in Blue View had ingelogd om aan de hand van die informatie te oordelen dat verdachte dus wederrechtelijk is binnengedrongen met behulp van een valse sleutel. De Hoge Raad wijst er niet alleen op dat verdachte op Blue View heeft ingelogd maar ook dat hij vervolgens gegevens over personen heeft bevraagd, heeft ingezien en overgenomen en aan derden (criminelen) heeft verstrekt. R.o. 2.4.1 zou zo kunnen worden begrepen dat uit deze gedragingen blijkt dat verdachtes reden (of doel) om in te loggen een andere was dan waarvoor hij mocht inloggen. Mede uit de handelingen na het inloggen blijkt dat hij misbruik maakte van zijn autorisatie en daarmee de wederrechtelijkheid van het toegang verwerven tot politiegegevens en de valsheid van zijn sleutel. Wat dus na het inloggen gebeurde is relevant voor het bewijs van wederrechtelijk binnendringen.
De nadruk op die gedragingen sluit niet zonder meer uit dat de Hoge Raad ook het wederrechtelijk vertoeven onder het bereik van art. 138ab lid 1 Sr brengt. Het gaat in r.o. 2.4.1 namelijk vooral om datgene wat de verdachte na het inloggen deed: naspeuringen verrichten, persoonsgegevens bevragen en gegevens inzien. Die handelingen zou ik op zichzelf geen binnendringen noemen in de zin van toegang verwerven, en evenmin overnemen, aftappen of opnemen (de gedragingen in het tweede lid van art. 138ab Sr), maar vertoeven in een geautomatiseerd werk nadat daarin is binnengedrongen en voordat gegevens worden overgenomen, afgetapt of opgenomen. Aanvaarding van een dergelijke lezing van art. 138ab Sr vind ik niet in de wetsgeschiedenis, en ook het rapport *Informatietechniek en strafrecht* (Den Haag: Staatsdrukkerij 1987) van de Commissie computercriminaliteit wijst er niet op dat wederrechtelijk vertoeven wordt begrepen in art. 138ab lid 1 Sr.

5.

Het arrest leert ons dat bij de vraag of een verdachte (een deel van) een geautomatiseerd werk wederrechtelijk is binnengedrongen gedragingen mogen worden betrokken die plaatsvonden nadat toegang is verworven tot het geautomatiseerde werk. De vraag rijst of dergelijke gedragingen op zichzelf altijd voldoende kunnen zijn voor een bewezenverklaring van wederrechtelijk binnendringen. Mijns inziens zou het enkele onbevoegd naspeuringen doen zonder dat uit feiten of omstandigheden duidelijk is geworden dat toegang is verworven om juist die naspeuringen te doen, niet voldoende moeten zijn om aan te nemen dat er sprake is van wederrechtelijk binnendringen met behulp van een valse sleutel. Wat in dat geval wordt vastgesteld is namelijk enkel het vertoeven in (een deel van) een geautomatiseerd werk. En het komt mij voor dat niet de Hoge Raad maar de wetgever moet bepalen of dergelijk gedrag op zichzelf strafbaar zou moeten worden gesteld (hetgeen thans volgens mij niet het geval is in art. 138ab en evenmin in art. 138c Sr). De onderhavige zaak leert ons misschien wel dat aan een dergelijke strafbaarstelling behoefte zou kunnen bestaan.

Voetnoten

[1.]
De volledige kwalificatie luidt: “medeplegen van enig geheim waarvan hij weet dat hij uit hoofde van zijn ambt en wettelijk voorschrift verplicht is het te bewaren, opzettelijk schenden, meermalen gepleegd en enig geheim waarvan hij weet dat hij uit hoofde van zijn ambt en wettelijk voorschrift verplicht is het te bewaren, opzettelijk schenden, meermalen gepleegd.”

[2.]
De volledige kwalificatie luidtt: “computervredebreuk, terwijl de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt en worden overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf en een ander overneemt, meermalen gepleegd.”

[3.]
De volledige kwalificatie luidt: “als ambtenaar een belofte aannemen, wetende dat deze hem gedaan wordt teneinde hem te bewegen om in zijn bediening iets te doen.”

[4.]
De volledige kwalificatie luidt : “van het plegen van witwassen een gewoonte maken.”

[5.]
De volledige kwalificatie luidtt: “een reisdocument voorhanden hebben, waarvan hij redelijkerwijs moet vermoeden, dat het vals of vervalst is, meermalen gepleegd.”

[12.]
Vgl. HR 25 mei 2010, ECLI:NL:HR:2010:BL5563.

[13.]
Wet van 27 juni 2018, *Stb.* 2018, 322, i.w.tr. op 1 maart 2019.

[14.]
Zie schriftuur onder 2.16 - 2.21.

[15.]
Art. 138c Sr bevat een lagere strafbedreiging dan art. 138ab Sr.

[16.]
Zie J. de Hullu, Materieel Strafrecht, achtste druk, Wolters Kluwer 2021, II.5.1.

[17.]
Kamerstukken II 1990/91, 21551, nr. 6, p. 31-32.

[18.]
Kamerstukken II 1990/91, 21551, nr. 6, p. 31.

[19.]
HR 20 mei 1986, ECLI:NL:HR:1986:AC9359, *NJ* 1987/130, rov. 5.1.

[20.]
HR 8 december 1992, ECLI:NL:HR:1992:ZC8478, *NJ* 1993/323.

[21.]
HR 20 december 2016, ECLI:NL:HR:2016:2892, *NJ* 2017/158 m.nt. N. Keijzer, rov. 2.3.4.

[22.]

Zie bijv. *Kamerstukken II* 1990/91, 21551, 6 (MvA), p. 8-9: “De strafrechtelijke bescherming van gegevens is daarom juist gezocht in de aansluiting bij de klassieke bescherming van gegevens: de bescherming van wat in de memorie van toelichting reeds is aangeduid als de huls (…) Vandaar ook de term computervredebreuk. Of gegevens worden ingezien dan wel gecopieerd is daarbij niet relevant. Niet de gegevens zijn beveiligd, doch de huls.” En p. 9: “Het gaat om de strafrechtelijke bescherming van de huls of de verpakking, niet van de gegevens zelf. Alleen op die wijze wordt de bestaande strafrechtelijke bescherming van gegevens op weliswaar gewijzigde technische gronden, doch juridisch-dogmatisch dezelfde gronden verwerkelijkt.”

[23.]
Kamerstukken II 1990/91, 21551, 6, p. 28-29: “Gemeenschappelijk is dat de onbelemmerde kennisneming van gegevens, ook al zijn deze niet voor de betrokkene bestemd, niet strafbaar is. Evenmin is van belang of de kennisneming per ongeluk plaatsvindt dan wel opzettelijk de situatie is opgezocht om van de betrokken gegevens kennis te nemen. Strafbaarheid ontstaat eerst daar waar doelbewust getroffen voorzieningen met het oog op geheimhouding worden omzeild, om aldus de kennelijk door de rechthebbende niet gewenste kennisneming door derden, toch te bewerkstelligen. In het begrip «binnendringen» wordt de opzet begrepen geacht.”

[24.]
Kamerstukken II 1989/90, 21551, 3, p. 15.

[25.]
Kamerstukken II 1989/90, 21551, 3, p. 17.

[26.]
Conclusie AG Knigge 28 september 2010, ECLI:NL:PHR:2011:BN9287, onder 49.

[27.]
Kamerstukken II 1990-1991, 21551, nr. 7 (Nota van wijziging), p. 4. Zie ook *Kamerstukken II* 1990/91, 21551, 6, p. 8: “Zo worden ook in het voorgestelde artikel 138a bepaalde vormen van binnendringen nader aangeduid, naast het noemen van de beveiligingsies [sic] in het algemeen.”

[28.]
Zie bijv. *Kamerstukken II* 2004/05, 26671, 7 (Tweede nota van wijziging), p. 32: “Mede met het oog op een zo krachtig mogelijke bestrijding van het verschijnsel «hacking» acht ik het daarom wenselijk geen beperking aan te brengen maar artikel 138a zodanig te herformuleren, dat in beginsel ieder opzettelijk en wederrechtelijk binnendringen in een computer(systeem) bestraft kan worden. Daarom stel ik voor de onderdelen a en b van artikel 138a, die thans nog als voorwaarde voor strafbaarheid zijn geformuleerd, te formuleren als voorbeelden van gevallen waarin sprake is van «binnendringen», door aan te geven dat in die gevallen in ieder geval sprake is van binnendringen in de zin van dit artikel. Daarmee wordt voor de jurisprudentie de nodige ruimte geschapen om ook andere methoden waarmee toegang wordt verworven, als binnendringen aan te merken.”

[29.]
Zoals naar voren komt in het onder 5.19. geciteerde stuk uit de Memorie van Antwoord bij het wetsvoorstel Computercriminaliteit I, *Kamerstukken II*, 1990/91, 21551, nr. 6, p. 30.

[30.]
Kamerstukken II 1998/99, 26671, 3, p. 32-33.

[31.]
Kamerstukken II 2015/16, 34372, nr. 3, p. 66.

[32.]
HR 20 december 2016, ECLI:NL:HR:2016:2892, *NJ* 2017/158, m.nt. N. Keijzer.

[33.]
Zie ook het onder de bewijsmiddelen op p. 11 van het arrest opgenomen “AMB257: proces-verbaal van bevindingen van 20 juni 2016 op ambtseed/belofte verbalisanten Boss en Aarts (p. 679- 713); […] Voor exporteren is geen aparte bevoegdheid nodig. […] Er is een waarschuwing opgenomen aan de gebruiker:….“het oneigenlijk gebruik dan wel misbruik van deze gegevens is ten strengste verboden. Daarnaast is het verstrekken van deze gegevens aan derden welke niet de vereiste autorisatie bezitten eveneens ten strengste verboden…… (pagina 700)”.